(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 704 785 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.04.1996 Bulletin 1996/14

(51) Int. Cl.[6]: **G06F 1/00**, G06F 12/14

(21) Application number: **95115068.9**

(22) Date of filing: **25.09.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **30.09.1994 JP 237673/94**
27.10.1994 JP 264199/94
02.11.1994 JP 269959/94

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku Tokyo 100 (JP)

(72) Inventors:
- **Saito, Makoto**
  Tama-shi, Tokyo (JP)
- **Momiki, Shunichi**
  Higashimurayama-shi, Tokyo (JP)

(74) Representative: **Neidl-Stippler, Cornelia, Dr.**
Patentanwälte Neidl-Stippler & Partner
Rauchstrasse 2
D-81679 München (DE)

(54) Data copyright management system

(57) A data copyright management system comprises a database for storing original data, a key control center for managing crypt keys, copyright management center for managing data copyrights, and a communication network for connecting these sections each other; data supplied from the database to users is encrypted and distributed, and the users decrypting the encrypted data by crypt keys obtained from the key control center or copyright management center to use the data.

To supply data to users, there are the following two methods: one for one-way supplying encrypted data to users by means of broadcasting or the like, and the other for two-way supplying encrypted data to users corresponding to users' requests.

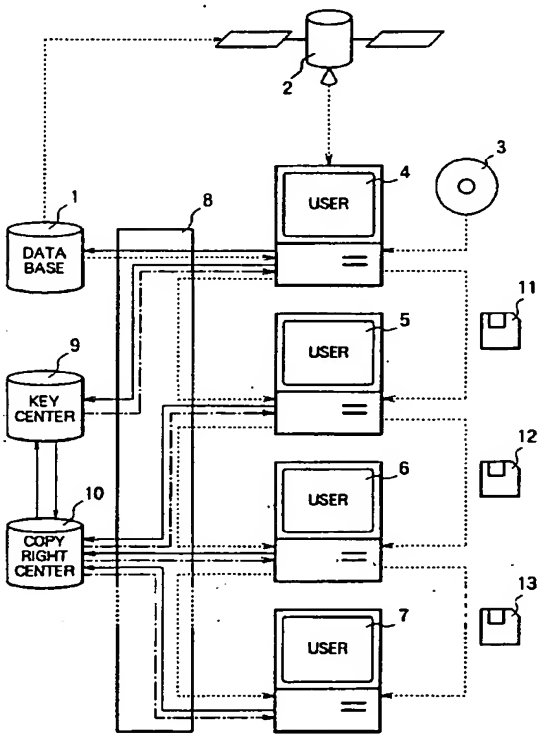
A crypt key system used for encrypting data uses a secret-key cryptosystem, a public-key cryptosystem or a cryptosystem combining a secret-key and a public-key and moreover, uses a copyright management program for managing data copyrights.

When a user stores, copies, or transfers data, the data is encrypted by a crypt key different from a crypt key used for supplying the data. The former crypt key is supplied from the key control center or from the copyright management center, or generated by the copyright management program.

Moreover, the present invention can be applied to a data copyright management system for using not only signal data but also a plurality of data supplied from a single database or a plurality of data supplied from a plurality of databases.

Furthermore, an apparatus to be used by the user to perform data copyright management is also proposed.

FIG. 1



EP 0 704 785 A2

Description

Field of the Invention

The present invention relates to a system for managing copyrights for using, storing, copying, editing, or transmitting digital data, particularly applicable to a multimedia system.

Background of the Invention

In information-oriented society of today, a database system has been spread in which various data values having independently been stored in each computer so far are mutually used by connecting computers by communication lines.

The information having been handled by the database system is classical type coded information which can be processed by a computer and has a small amount of information or monochrome binary data like facsimile data at most. Therefore, the database system has not been able to handle data with an extremely large amount of information such as a natural picture and a motion picture.

However, while the digital processing technique for various electric signals develops, development of the digital processing art for a picture signal other than binary data having been handled only as an analog signal is progressed.

By digitizing the above picture signal, a picture signal such as a television signal can be handled by a computer. Therefore, a "multimedia system" for handling various data handled by a computer and picture data obtained by digitizing a picture signal at the same time is noticed as a future technique.

Because picture data includes an overwhelmingly large amount of information compared to character data and audio data, it is difficult to directly store or transmit the picture data or apply various processings to the picture data by a computer.

Therefore, it has been considered to compress or expand the picture data and several standards for compressing or expanding picture data have been prepared. Among those standards, the following standards have been prepared so far as common standards: JPEG (Joint Photographic image coding Experts Group) standard for a still picture, H.261 standard for a video conference, MPEG1 (Moving Picture image coding Experts Group 1) standard for storing pictures, and MPEG2 corresponding to the present telecast and the high-definition telecast.

Real-time processing of digital picture data has been realized by these techniques.

Because hitherto widely-spread analog data is deteriorated in quality whenever storing, copying, editing, or transmitting it, the editing of a copyright produced due to the above operation has not been a large problem. However, because digital data is not deteriorated in quality after repeatedly storing, copying, editing, or transmitting it, the editing of a copyright produced due to the above operation is a large problem.

Because there is not hitherto any exact method for dealing with a copyright for digital data, the copyright is handled by the Copyright Act or contracts. Even in the Copyright Act, compensation money for a digital-type sound- or picture-recorder is only systematized.

Use of a database includes not only referring to the contents of the database but also normally effectively using the database by storing, copying, or editing obtained data. Moreover, it is possible to transmit edited data to another person via on-line by a communication line or a proper recording medium. Furthermore, it is possible to transmit the edited data to the database to enter it as new data.

In an existing database system, only character data is handled. In a multimedia system, however, audio data and picture data which are originally analog data are digitized and formed into a database in addition to the data such as characters which have been formed into a database so far.

Under the above situation, how to deal with a copyright of data formed into a database is a large problem. However, there has not been adequate copyright management means for solving the problem so far, particularly copyright management means completed for secondary utilization of the data such as copying, editing, or transmitting of the data.

The inventor of the present invention et al. proposed a system for managing a copyright by obtaining a permit key from a key control center via a public telephone line through Japanese Patent Laid-Open No. 46419/1994 and Japanese Patent Laid-Open No. 141004/1994 and moreover, proposed an apparatus for managing the copyright through Japanese Patent Laid-Open No. 132916/1994.

Moreover, they proposed a copyright management method for primary utilization of digital data such as display (including process to sound) or storage of the digital data in a database system including real-time transmission of a digital picture and secondary utilization of the digital data such as copying, editing, or transmitting of the digital data by further developing the above prior invention through Japanese Patent Application No. 64889/1994.

The database copyright management system of the prior applications use anyone or some of a program for managing a copyright, copyright information, and a copyright management message in addition to a use permit key corresponding to a requested use in order to manage the copyright.

The copyright management message is displayed when utilization infringing the user's request or authorized contents is found to give caution or warning to a user and the copyright management program performs monitoring and management so that utilization infringing the user's request or authorized contents is not performed.

There are cases in which all of a copyright management program, copyright information and a copyright

management message is supplied together with each permit key respectively, the whole of them is supplied together with data, and part of them is supplied together with the permit key and other part is supplied together with the data.

The data, the permit key, the copyright management message, the copyright information, or the copyright management program has the following three cases: a case in which it is transmitted by being encrypted and it is decrypted when it is used, a case in which it is transmitted by being encrypted and remains in encrypted except being decrypted only when it is displayed, and a case in which it is not encrypted at all.

Summary of the Invention

This application provides a data copyright management system realized by embodying the data copyright management method of the prior application proposed in the above Japanese Patent Application No. 64889/1994.

The data copyright management system of the present invention comprises a database for storing original data, a key control center for managing a crypt key, a copyright management center for managing a data copyright, and a communication network for connecting the above sections each other, in which data supplied to a user from the database is encrypted and the user uses the data after decrypting the data with a crypt key obtained from the key control center or the copyright management center.

There are the following two methods for supplying data to a user: a method for one-way supplying encrypted data to the user such as by broadcasting and a method for two-way supplying encrypted data to the user in accordance with a user's request.

A cryptographic key system used for encryption of data uses a secret-key cryptosystem, a public-key cryptosystem, or a system constituted by combining a secret-key and a public-key and moreover uses a copyright management program for managing a data copyright.

When a user stores, copies, or transmits data, the data is encrypted again by a crypt key, which is supplied from the key control center or from the copyright management center, or generated by the copyright management program.

Moreover, the present invention can be applied to a data copyright management system for using not only a single data value but also a plurality of data values supplied from a single database or a plurality of data values supplied from a plurality of databases.

Furthermore, an apparatus to be used by a user is also proposed in order to perform data copyright management.

Brief Description of the Drawings

Figure 1 illustrates a data copyright management system for embodiments 1, 2, and 3 of the present invention;

Figure 2 illustrates a data copyright management system of embodiment 4 of the present invention;

Figure 3 illustrates a data copyright management system for embodiments 5, 6, and 7 of the present invention;

Figure 4 illustrates a data copyright management system for embodiments 8, 9, 10 and 11 of the present invention;

Figure 5 illustrates a data copyright management system for embodiments 12 and 13 of the present invention;

Figure 6 is an illustration for data editing;

Figure 7 is an illustration showing a digital cash system;

Figure 8 illustrates a digital cash system for embodiments 17 and 18 of the present invention;

Figure 9 illustrates a video conference system for embodiment 19 of the present invention; and

Figure 10 illustrates an embodiment of a user terminal used for the data copyright management system of the present invention.

Detailed Description of the Preferred Embodiments

Though the present invention is described below, general description is made for cryptography at first.

The cryptography includes a secret-key cryptosystem and a public-key crypto system.

The secret-key cryptosystem is a cryptosystem using the same crypt key for encryption and decryption. While this cryptosystem requires only a short time for encryption or decryption, the secret-key is found, and thus, the cryption may be cryptanalized.

The public-key cryptosystem is a cryptosystem in which a key for encryption is open to the public as a public-key and a key for decryption is not open to the public. The key for encryption is referred to as a public-key and the key for decryption is referred to as a private-key. To use this cryptosystem, it is necessary that a party for transmitting information encrypts the information with a public-key of a party for receiving the information and the party for receiving the information decrypts the information with a private-key not open to the public. While this cryptosystem requires relatively a long time for encryption or decryption, the private-key can hardly be found and it is very difficult to cryptanalyze the cryption.

In the cryptography, a case of encrypting a plaintext M with a crypt key K to obtain a cryptogram C is expressed as

$$C = E(K, M)$$

and a case of decrypting the cryptogram C with the cryptographic key K to obtain the plaintext M is expressed as

$$M = D(K, C).$$

The cryptosystem used for the present invention uses a secret-key cryptosystem in which the same secret-key Ks is used for encryption and decryption, and a public-key cryptosystem in which a public-key Kb is used for encryption of a plaintext and a private-key Kv is used for decryption of a cryptogram.

[Embodiment 1]

Figure 1 shows the first embodiment of the data copyright management system of the present invention. The first embodiment uses the secret-key system as a cryptosystem.

In the case of the embodiment in Figure 1, reference numeral 1 represents a database in which text data, binary data serving as a computer graphic display or a computer program, digital audio data, and digital picture data are stored by being encrypted, 2 represents a space satellite such as a communications satellite or a broadcasting satellite, 3 represents a data recorder such as a CD -ROM or a flexible disk, 8 represents a communication network such as a public telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise, 4 represents a primary user terminal, and 9 represents a key control center for managing a secret-key, and 10 represents a copyright management center for managing a data copyright.

Reference numerals 5, 6, and 7 represent a secondary user terminal, a tertiary user terminal, and n-order user terminal respectively, and 11, 12, and 13 represent a secondary disk, tertiary disk, and n-order disk serving as a recording medium such as a flexible disk or CD-ROM respectively. The symbol "n" represents an optional integer. When "n" is larger than 4, a corresponding user terminal and a corresponding disk are arranged between the tertiary user terminal 6 and the n-order user terminal 7 and between the tertiary disk 12 and the n-order disk 13 respectively.

On the above arrangement, the database 1, key control center 9, copyright management center 10, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-order user terminal 7 are connected to the communication network 8.

In this figure, the path shown by a broken line is a path of encrypted data, a path shown by a solid line is a path of requests from each user terminal, and a path shown by a one-dot chain line is a path through which authorization information corresponding to a utilization request and a secret-key are transferred.

Moreover, each user who uses this system is previously entered in the database system. When the user is entered in the system, a database utilization software is given to the user. The database utilization software includes not only normal communication software such as a data communication protocol but also a program for running a copyright management program.

Original data M0 of text data, binary data as a computer graphic display or computer program, digital audio data, or digital picture data stored in the database 1 or data recording medium 3 is one-way supplied to the primary user terminal 4 via the satellite 2 or recording medium 3. In this case, the data is encrypted with a first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0).$$

Even if data provided with advertisement to be offered free of charge, it is necessary to be encrypted in order to protect the copyright.

It is disclosed in the above described Japanese Patent Application No. 64889/1994 which is the prior application that the data utilization includes not only displaying of data which is the most basic usage but also storing, editing, copying, and transmitting of the data, a use permit key is prepared which corresponds to one or several forms of use, and its management is executed by the copyright management program.

Moreover, it is described there that data is encrypted again by the copyright management program for use such as storing, copying, editing and transmitting of the data other than displaying of the data and displaying for editing the data.

In other words, the data whose copyright is claimed is encrypted to be distributed, and only when the data is displayed or displayed for editing the data in a user terminal having a copyright treatment function, the data is decrypted to a plaintext.

This embodiment uses the method described in the prior application.

A primary user who desires primary utilization of the supplied encrypted data Cm0ks1 requests for primary utilization of the encrypted original data Cm0ks1 by designating the original data name or the original data number to the key management center 9 via the communication network 8 from the primary user terminal 4. In this case, the primary user must present information Iu1 for primary user to the key management center 9.

The key management center 9 receiving the primary utilization request from the primary user terminal 4 transfers the first secret-key Ks1 for decrypting the encrypted original data Cm0ks1 obtained from the database 1 by the primary user and the second secret-key Ks2 for re-encrypting the decrypted original data M0 or edited data M1 from the original data, together with a copyright management program P via the communication network 8 to the primary user terminal 4.

In the primary user terminal 4 receiving the first secret-key Ks1 as a decryption key and the second secret-key Ks2 as an encryption/decryption key, the encrypted original data Cm0ks1 is decrypted by using the copyright management program P and the first secret-key Ks1

$$M0 = D(Ks1, Cm0ks1)$$

to use the decrypted original data M0 directly or data M1 as edited.

When the data M which is the original data M0 or edited data M1 is stored in a memory or a built-in hard disk drive of the primary user terminal 4, only the primary user can use the data. However, when the data M is copied to the external recording medium 11 such as a flexible disk or transmitted to the secondary user terminal 5 via the communication network 8, a problem of a copyright due to secondary utilization occurs.

When the original data M0 obtained by a primary user is directly copied and supplied to a secondary user, the copyright of the primary user is not effected on the data M0 because the original data M0 is not modified at all. However, when the primary user produces new data M1 by editing the obtained data or by using means such as combination with other data, the copyright of the primary user, i.e., secondary exploitation right occurred from secondarily utilizing original data, is effected on the data M1.

Similarly, when a secondary user produces new data M2 by editing the original data M0 or edited data M1 obtained from the primary user by means such as combination of other data, the copyright of the secondary user; i.e., secondary exploitation right on the secondary user is also effected.

In this embodiment, to correspond to the problem of the copyright, the data M is encrypted by the second secret-key Ks2 using the copyright management program P when the data M is stored, copied, or transmitted. Thereafter, in the primary user terminal 4, the data M is decrypted and encrypted by the second secret-key Ks2:

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2).$$

It is free in principle that the primary user displays and edits data to obtain edited data. In this case, however, it is possible to limit the repetitions of the operation by the copyright management program.

When the data M is copied to the external recording medium 11 or transmitted via the communication network 8, the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 are disused by the copyright management program P. Therefore, when reusing the data M, the primary user requests for utilization of the data M to the key control center 9 to again obtain the second secret-key Ks2.

The fact that the user receives the regrant of the second secret-key Ks2 represents secondary utilization of data in which the data M has been copied to the external recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8. Therefore, the fact is entered in the copyright management center 10 from the key control center 9 and subsequent secondary utilization comes possible.

The data M is moved from the primary user terminal 4 to the secondary user terminal 5 by the external recording medium 11 or the communication network 8. When the data M is copied to the external recording medium 11 or transmitted via the communication network 8, it is encrypted by the second secret-key Ks2.

When the data M is copied to the external recording medium 11 and transmitted via the communication network 8, the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 are disused. In this case, uncrypted primary user information Iu1 is added to the encrypted data Cmks2 stored in the primary user terminal 4 and when the encrypted data Cmks2 is transmitted to a secondary user, the primary user information Iu1 is also transferred.

A secondary user who desires secondary utilization of the encrypted data Cmks2 copied or transmitted from a primary user must designate original data name or data number to the copyright management center 10 via the communication network 8 by the secondary user terminal 5 and also present the secondary user information Iu2 to request for secondary utilization of the data Cmks2 to the center 10. In this case, the secondary user further presents the uncrypted primary user information Iu1 added to the encrypted data Cmks2 in order to clarify the relationship with the primary user.

The copyright management center 10 confirms that the primary user has received a regrant of the second secret-key Ks2 for secondary-utilizing the data, in accordance with the presented primary user information Iu1 and then, transfers the second secret-key Ks2 serving as a decryption key and the third secret-key Ks3 serving as an encryption/decryption key to the secondary user terminal 5 via the communication network 8.

In the secondary user terminal 5 receiving the second secret-key Ks2 and the third secret-key Ks3, the encrypted data Cmks2 is decrypted using the second secret-key Ks2 by the copyright management program P

$$M = D(Ks2, Cmks2)$$

and is secondarily utilized such as being displayed or edited.

In this embodiment, the key control center 9 processes a primary utilization requests and the copyright management center 10 processes a secondary utilization requests. While the data M supplied to a primary user is encrypted by the first secret-key Ks1, the data M supplied to a secondary user is encrypted by the second secret-key Ks2. Moreover, the first secret-key Ks1 and the second secret-key Ks2 are transferred to the primary user as crypt keys from the key control center 9.

Therefore, if the secondary user, instead of the primary user, falsely requests for primary utilization to the key control center 9, the first secret-key Ks1 for decryption and the second secret-key Ks2 for encryption/decryption are transferred to the secondary user. However, the secondary user cannot decrypt the encrypted data Cmks2 by using the first secret-key Ks1 transferred as a decryption key.

Therefore, it is impossible to falsely request for data utilization and resultingly, not only the original copyright of data but also the copyright of the primary user on the data are protected.

When storing, copying, or transmitting of the data M other than displaying and displaying for editing is performed in the secondary user terminal 5, the data M is encrypted using the third secret-key Ks3 by the copyright management program P and thereafter, the data is decrypted and encrypted by the third secret-key Ks3:

$$Cmks3 = E(Ks3, M)$$

$$M = D(Ks3, Cmks3).$$

Moreover, it is free in principle that a secondary user displays and edits data to obtain the edited data M2. In this case, it is possible to limit the repetitions of the operation by the copyright management program P.

When the data M is copied to the external recording medium 12 or transmitted via the communication network 8, the second secret-key Ks2 and the third secret-key Ks3 in the secondary user terminal 5 are disused by the copyright management program P. Therefore, when reusing the data M, the secondary user requests for the utilization of the data to the copyright management center 10 to again obtain the third secret-key Ks3.

The fact that the secondary user receives a regrant of the third secret-key Ks3 represents secondary utilization of data in which the data M has been copied to the external recording medium 12 or transmitted to the tertiary user terminal 6 via the communication network 8. Therefore, the fact is entered in the copyright management center 10 and allows the secondary user for subsequest data use.

The data M is moved from the secondary user terminal 5 to the tertiary user terminal 6 by the external recording medium 12 or by the communication network 8. When the data M is copied to the external recording medium 12 or transmitted via the communication network 8, it is encrypted by the third secret-key Ks3.

When the data M is copied to the external recording medium 12 or transmitted to the tertiary user terminal 6 via the communication network 8, the second secret-key Ks2 and the third secret-key Ks3 in the secondary user terminal 5 are disused. In this case, the uncrypted secondary user information Iu2 is added tothe encrypted data Cmks3 stored in the secondary user terminal 5, and when the encrypted data Cmks3 is transmitted to a tertiary user, the secondary user information Iu2 is also transferred.

In adding each user information to data, there are two cases: a case in which every information is added to data whenever it is copied or transmitted; and another in which the history updated whenever the data is copied or transmitted is stored in the copyright management center.

A tertiary user who desires tertiary utilization of the encrypted data Cmks3 copied or transmitted from the secondary user must designate original data name or number to the copyright management center 10 from a tertiary user terminal 6 via the communication network 8 and also presents the tertiary user information Iu3 to request for tertiary utilization of the data. In this case, the tertiary user further presents the uncrypted secondary user information Iu2 added to the encrypted data Cmks3 in order to clarify the relationship with the secondary user.

The copyright management center 10 confirms that the secondary user has received a regrant of the third secret-key Ks3 for tertiary-utilizing the data, in accordance with the presented secondary user information Iu2 and then, transfers the third secret-key Ks3 serving as a decryption key and the fourth secret-key Ks4 serving as an encryption/decryption key to the tertiary user terminal 6 via the communication network 8.

In the tertiary user terminal 6 receiving the third secret-key Ks3 and the fourth secret-key Ks4, the encrypted data Cmks3 is decrypted using the third secret-key Ks3 by the copyright management program P

$$M = D(Ks3, Cmks3)$$

and is tertiarily utilized such as being displayed or edited.

In this embodiment, the data M supplied to a primary user is encrypted by the first secret-key Ks1 and the data M supplied to a secondary user is encrypted by the second secret-key Ks2, and the data M supplied to a tertiary user is encrypted by the third secret-key Ks3.

Therefore, if the tertiary user, instead of the primary user, falsely requests for primary utilization to the key control center 9, the first secret-key Ks1 for decryption and the second secret-key Ks2 for encryption/decryption are transferred to the tertiary user. However, it is impossible to decrypt the encrypted data Cmks3 by the first secret-key Ks1 transferred as a decryption key.

Moreover, if the tertiary user, instead of the secondary user, falsely requests for secondary utilization to the key control center 9, the second secret-key Ks2 and the third secret-key Ks3 are transferred to the tertiary user as a decryption key and an encryption/decryption key respectively. However, it is impossible to decrypt the encrypted data CmKs3 by the second secret-key Ks2 transferred as a decryption key.

Therefore, it is impossible to falsely request for data utilization. As a result, not only the original copyright of the data but also the copyrights of the primary and secondary users on the data are protected.

The same procedure is applied to quaternary and subsequent utilization.

In the above described embodiment, the database 1, key control center 9, and copyright management center 10 are separately arranged. However, it is not always necessary to arrange them separately. It is also possible to aet all of or proper two of them integrally.

Moreover, it is also possible to request for a regrant of a secondary crypt key from the primary user not to the

key control center 9 as described in the above embodiment but to the copyright management center 10.

[Embodiment 2]

Then, embodiment 2 is described below. Though the structure of this embodiment is mostly the same as that of the first embodiment, a copyright management program and, if circumstances require, first and second secret-keys are encrypted and supplied.

Also in the case of this embodiment, similarly to the case of the first embodiment, original data is encrypted and supplied one-way to a user from a single database and the user selects necessary data out of the original data.

Because the system structure used for the second embodiment is the same as that of embodiment 1 shown in Figure 1, description of the system structure is omitted.

In his embodiment, the original data M0 stored in the database 1 is supplied one-way to the primary user terminal 4 via the satellite 2, recording medium 3, or communication network 8. The data M0 is encrypted by the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0).$$

A primary user who desires primary utilization of the supplied encrypted data Cm0ks1 requests for the primary utilization of the encrypted original data Cm0ks1 to the key control center 9 by using the primary user terminal 4 and designating an original data name or an original data number via the communication network 8. In this case, the primary user must present the primary user information Iu1 to the key control center 9.

The key management 9 receiving the request of the primary utilization of the encrypted original data Cm0ks1 generates a secret-key Ksu1 unique to the primary user using the primary user information Iu1 and transfers it to the copyright management center 10.

The copyright management center 10 receiving the primary user unique secret -key Ksu1 encrypts the copyright management program P by using the primary user unique secret-key Ksu1

$$Cpksu1 = E(Ksu1, P)$$

and transfers an encrypted copyright management program Cpksu1 to the key control center 9. The encrypted copyright management program Cpksu1 thus generated is inherent in the primary user.

The key control center 9 transfers the first secret-key Ks1 for decryption and the second secret-key Ks2 for decryption/encryption to the primary user terminal 4 via the communication network 8, together with the encrypted copyright management program Cpksu1 received from the copyright management center 10.

In the primary user terminal 4 receiving the encrypted copyright management program Cpksu1, first secret-key Ks1, and second secret-key Ks2, database system software S previously distributed generates a primary user unique secret-key Ksu1 in accordance with the primary user information Iu1:

$$Ksu1 = S(Iu1),$$

and an encrypted copyright management program Cpksu1 is decrypted by the generated primary user unique secret-key Ksu1:

$$P = D(Ksu1, Cpksu1),$$

the encrypted original data Cm0ks1 is decrypted by the first secret-key Ks1 using the copyright management program P:

$$M0 = D(Ks1, Cm0ks1),$$

and the decrypted original data M0 directly or edited data M1 is used.

When the data M as the original data M0 or edited data M1 is stored, copied, or transmitted, it is encrypted by the copyright management program P using the secret-key Ks2, and thereafter the data M is decrypted and encrypted in the primary user terminal 4 by the second secret-key Ks2:

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2).$$

When the data M is copied to the external recording medium 11 or the data is transmitted via the communication network 8, the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 are disused by the copyright management program P. Therefore, when the primary user uses the data M again, the user requests for utilization of the data M to the key control center 9 to again obtain the second secret-key Ks2.

The fact that the primary user receives a regrant of the second secret-key Ks2 represents secondary utilization of data in which the data M has been copied to the external recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8. Therefore, this is entered in the copyright management center 10 from the key control center 9 and thereafter, secondary utilization of the data can be made.

The data M is moved from the primary user terminal 4 to the secondary user terminal 5 by the external recording medium 11 or by the communication network 8.

When the data M is copied to the external recording medium 11 or transmitted via the communication network 8, it is encrypted by the second secret-key Ks2.

When the data M is copied to the external recording medium 11 or transmitted via the communication network 8, the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 are disused. In this case, the uncrypted information Iu1 on a primary user is added to the encrypted data Cmks2 stored in the

primary user terminal 4. Therefore, when the encrypted data Cmks2 is transmitted to a secondary user, the primary user information Iu1 is also transferred to the user.

A secondary user who desires secondary utilization of the encrypted data Cmks2 copied or transmitted from the primary user must designate a data name or number added to the original data to the copyright management center 10 via the communication network 8 by the secondary user terminal 5 and also presents a secondary user information Iu2 to request for the secondary utilization of the data to the center 10. In this case, the secondary user further presents the uncrypted primary user information Iu1 added to the encrypted data Cmks2 in order to clarify the relationship with the primary user.

The copyright management center 10 confirms that the primary user has received a regrant of the secondary secret-key Ks2 for secondary-utilizing the data in accordance with the presented primary user information Iu1 and then, generates a secret-key Ksu2 unique to the secondary user in accordance with the presented secondary user information Iu2.

The copyright management center 10 encrypts the copyright management program P by the secondary user unique secret-key Ksu2

$$Cpksu2 = E(Ksu2, P)$$

and transfers the encrypted copyright management program Cpksu2, second secret-key Ks2 serving as a decryption key, and third secret-key Ks3 serving as an encryption/decryption key via the communication network 8 to a secndary user terminal 5.

Moreover, the information Iu1 for a primary user may be added to the encrypted copyright management program Cpksu2.

In the secondary user terminal 5 receiving the second secret-key Ks2 and the third secret-key Ks3, database utilization software generates a secondary user unique secret-key Ksu2 in accordance with the secondary user information Iu2

$$Ksu2 = S(Iu2),$$

and an encrypted copyright management program Cpksu2 by the generated secondary user unique secret-key Ksu2

$$P = D(Ksu2, Cpksu2),$$

the encrypted original data Cmks2 is decrypted by the second secret-key Ks2 using the decrypted copyright management program P

$$M = D(Ks2, Cmks2),$$

and the decrypted data M directly or by editing it is used.

Thus, by generating a crypt key unique to a user in accordance with the information of the user requests for utilization, and encrypting a copyright management program by the generated user unique crypt key, the safety of a data copyright management system is improved.

Moreover, by encrypting each secret-key to be supplied to a user, using the user unique crypt key, the safety of the data copyright management system can further be improved.

[Embodiment 3]

Furthermore, as still another method for corresponding to the problem of a copyright caused when the data M is copied to the external recording medium 11 or transmitted via the communication network 8 in the system shown in Figure 1, it is possible to limit the primary utilization request by a user of the primary user terminal 4 to only for permits of displaying, storing and editing so that other utilization such as copying and transmitting cannot be authorized except by separate requests, and disuse the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 when the data M is copied to the external recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8.

Thus, it is possible that the copyright management center 10 further securely grasps copying or transmitting of the data M.

[Embodiment 4]

Figure 2 shows a structure of embodiment 4 of the data copyright management system of the present invention.

In the case of the system shown in Figure 1, encrypted data is one-way supplied via the satellite 2, recording medium 3, or communication network 8. In the case of embodiment 2, however, encrypted data is two-way supplied in accordance with a request from the primary user 4.

This embodiment uses the public-key cryptosystem as a crypt key system.

It is matter of course that embodiment 2 can be applied when using a satellite broadcast, ground wave broadcast, CATV broadcast or a recording medium other than a database as data supply means provided with advertisement requiring no charge or encryption .

In the system shown in Figure 2 similarly to the system shown in Figure 1, reference numeral 1 represents a database, 4 represents a primary user terminal, 5 represents a secondary user terminal, 6 represents a tertiary user terminal, and 7 represents an n-order user terminal.

And 14 represents a secondary copyright management center, 15 represents a tertiary copyright management center, 16 represents an n-order copyright management center, 8 represents a communication network such as a public telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise.

On the above arrangement, the database 1, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, n-order user terminal 7, secondary copyright management center 14, tertiary copyright management center 15, and n-order copyright management center 16 are connected to the communication network 8 and also they can be connected each other.

In Figure 2, a path shown by a broken line represents a path for encrypted data, a path shown by a solid line represents a path of requests from each user terminal, a path shown by a one-dot chain line represents a path through which authorization information sent from each database corresponding to a utilization request and a crypt key are transferred, and a path shown by a two-dot chain line represents a path through which copyright information is transferred from the database or each copyright management center database to a next-order copyright management center database.

Each user who uses this system is previously entered in a database system and in this time, database utilization software is provided him. The database utilization software includes a program for decrypting an encrypted copyright management program in addition to normal communication software such as data communicating protocol.

To use the database 1, a primary user must prepare primary-user authentication data Au1, a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2, and a second private-key Kv2 corresponding to the second public-key Kb2, and accesses the database 1 from the primary user terminal 4 via the communication network 8.

The database 1 receiving the primary-user authentication data Au1, first public-key Kb1 and second public-key Kb2 from the primary user confirms the primary-user authentication data Au1 and transfers the confirmed primary-user authentication data Au1 to the secondary copyright management center 14 as the primary user information Iu1.

The database 1 prepares two secret-keys, that is, the first secret-key Ks1 and the second secret-key Ks2. The two secret-keys may be prepared by using the key control center 9 of embodiment 1 shown in Figure 1.

In the prepared first secret-key Ks1 and second secret-key Ks2, the second secret-key Ks2 is also previously transferred to the copyright management center 14.

As the result of the above transfer, the primary user information Iu1 corresponding to primary utilization, original copyright information Ic and the second secret-key Ks2 are stored in the copyright management center 14. In this case, the original copyright information Ic is used for copyright royalties distribution.

When a primary user who desires data utilization accesses the database 1 from the primary user terminal 4, a data menu is transferred to him. In this case, information for charges may be displayed together with the data menu.

When the data menu is transferred, the primary user retrieves in the data menu to select the data M. In this case, the original copyright information Ic of the selected data M is transmitted to the copyright management center 14.

The original data M0 is read out of the database 1 in accordance with a request of a primary user. The read original data M0 is encrypted by the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0).$$

The encrypted data Cm0ks1 is provided with the uncrypted original copyright information Ic.

The first secret-key Ks1 is encrypted by the first public-key Kb1 and the second secret-key Ks2 is encrypted by the second public-key kb2:

$$Cks1kb1 = E(Kb1, Ks1)$$

$$Cks2kb2 = E(Kb2, Ks2).$$

While the copyright management program P is also encrypted by the second public-key Ks2:

$$CpKs2 = E(Ks2, P),$$

the copyright management program P must not always be encrypted by the second secret-key Ks2 but it may be encrypted by any other proper crypt key.

The encrypted original data Cm0ks1, encrypted copyright management program Cpks2, and two encrypted secret-keys Cks1kb1 and Cks2kb2 are transferred to the primary user terminal 4 via the communication network 8, and charged, if necessary.

It is possible to store the encrypted copyright management program Cpks2 such as in a ROM in the user terminal 4 instead of being supplied from the database 1.

The primary user receiving the encrypted original data Cm0ks1, two encrypted secret-keys Cks1kb1 and Cks2kb2, and encrypted copyright management program Cpks2 from the database 1 decrypts the encrypted first secret-key Cks1kb1 by the database utilization software using the first private-key Kv1 corresponding to the first public-key Kb1:

$$Ks1 = D(Kv1, Cks1kb1),$$

and decrypts the encrypted second secret-key Cks2kb2 using the second private-key Kv2 corresponding to the second public-key Kb2:

$$Ks2 = D(Kv2, Cks2kb2).$$

And the primary user decrypts the encrypted copyright management program Cp ks2 using the decrypted second secret-key Ks2:

$$P = D(Ks2, Cpks2).$$

Finally, the primary user decrypts the encrypted data Cm0ks1 by the decrypted copyright management program P usimg the decrypted first secret-key Ks1:

$$M0 = D(Ks1, Cm0ks1)$$

and uses the decrypted original data M0 directly or data M1 as edited.

As described above, the first private-key Kv1 and second private-key Kv2 are crypt keys prepared by the primary user but not opened to others. Therefore, even if a third party obtains the data M, it is impossible to use the encrypted data M by decrypting it.

Thereafter, to store, copy, or transmit the data M as the original data M0 or the edited data M1, it is encrypted and decrypted by the second secret-key Ks2:

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2).$$

The decrypted second secret-key Ks2 is thereafter used as a crypt key for encrypting/decrypting data when storing, copying, or transmitting the data.

The first private-key Kv1 and second private-key Kv2, the first secret-key Ks1 and second secret-key Ks2, the data M, the copyright management program P, the original copyright information Ic, and also the original cpyright information Ic and secondary cpyright information Ic1 for information of the primary user and edited date and time when edited the data by the primary user are stored in the primary user terminal 4.

Moreover, it is further protected by attaching the copyright information Ic1 to the data as copyright information label, and adding the digital signature.

The encrypted data Cmks2 is encrypted to be distributed. Since the copyright information label provides a clue to obtain the second secret-key Ks2 which is the key for decryption, the second secret key Ks2 cannot be procured in the case where the copyright information label is removed from the encrypted data Cmks2.

When the encrypted data Cmks2 is stored in the primary user terminal 4, the second secret-key Ks2 is stored in the terminal 4. However, when the encrypted data Cmks2 is not stored in the primary user terminal 4 but is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8, the second secret-key Ks2 is disused in order to disable subsequent utilization of the data in the primary user terminal 4.

In this case, it is possible to set a limitation for repetitions of copying or transmitting of the data so that the second secret-key Ks2 is not disused within limited repetions of copying and transmitting of the data.

A primary user who is going to copy the data M to the external recording medium 11 or transmit the data M via the communication network 8 must prepare the second secret-key Ks2 to encrypt the data M by this second secret-key Ks2 before copying or transmitting the data:

$$Cmks2 = E(Ks2, M).$$

The uncrypted original copyright information Ic and primary-user copyright information Ic1 are added to the encrypted data Cmks2.

Before using a database, a secondary user, similar to the primary user, prepares authentication data Au2 for authenticating the secondary user, a third public-key Kb3 and a third private-key Kv3 corresponding to the third public-key Kb3, a fourth public-key Kb4, and a fourth private-key Kv4 corresponding to the fourth public-key Kb4.

A secondary user who desires secondary utilization of the copied or transmitred encrypted data Cmks2 must designate original data name or number to the secondary copyright management center 14 to request for secondary utilization to the center 14 from the secondary user terminal 5 via the communication network 8. In this time, the secondary user also transfers the third public-key Kb3 and the fourth public-key Kb4 as well as the secondary user authentication data Au2, original copyright information Ic and primary user copyright information Ic1.

The secondary copyright management center 14 receiving the secondary utilization request from the secondary user confirms the secondary-user authentication data Au2, and transfers confirmed secondary-user authentication data Au2 to the tertiary copyright management center 15 as secondary user information.

When the secondary copyright information Ic1 of the primary user is transferred, the secondary copyright information Ic1 is inquired to the secondary copyright center 14, and then, it recognizes the secondary copyright information Ic1 to be transferred to the tertiary copyright management center 15.

The secondary copyright management center 14 prepares a third secret-key Ks3. The third secret-key Ks3 can also be prepared by using the key control center 9 shown in embodiment 1.

The prepared third secret-key Ks3 is transferred to and stored in the tertiary copyright management center 15.

As the result of the above transfer, primary user copyright information Ic1, primary user information Iu1, original copyright information Ic, secondary user information Iu2, and third secret-key Ks3 are stored in the tertiary copyright management center 15. The primary user copyright information Ic1, and primary user information Iu1 are used for copyright royalties distribution.

Hereafter similarly, copyright information for secondary exploitation right Icn-1 of (n-1)-order user, primary user information Iu1, original copyright information Ic, n-order user information Iun, and n-th secret-key Ksn are stored in n-order copyright management center 16.

The primary user information Iu1, original copyright information Ic and second secret-key Ks2 are read out of the secondary copyright management center 14. The original copyright information Ic is used for copyright royalties distribution.

The read second secret-key Ks2 and third secret-key Ks3 are encrypted by the third public-key Kb3 and fourth public-key Kb4 of the secondary user respectively:

$$Cks2kb3 = E(Kb3, Ks2)$$

$$Cks3kb4 = E(Kb4, Ks3).$$

The copyright management program P is encrypted by the third secret-key Ks3 and the third secret-key Ks3 is encrypted by the fourth public-key Kb4:

$$Cpks3 = E(Ks3, P)$$

$$Cks3kb4 = E(Kb4, Ks3).$$

The encrypted copyright management program Cpks3, encrypted second secret-key Cks2kb3, and encrypted third secret-key Cks3kb4 are transferred to the secondary user terminal 5 via the communication network 8. In this case, charging is performed, if necessary.

The secondary user receiving two encrypted secret-keys Cks2kb3 and Cks3kb4 and the encrypted copyright management program Cpks3 from the secondary copyright management center 14 decrypts the encrypted second secret-key Cks2kb3 by the third private-key Kv3, and decrypts the encrypted third secret-key Cks3kb4 by the fourth private-key Kv4 corresponding to the fourth public-key Kb4, using the database utilization software:

$$Ks2 = D(Kv3, Cks2kb3)$$

$$Ks3 = D(Kv4, Cks3kb4).$$

The encrypted copyright management program Cpks3 is decrypted by the decrypted third secret-key Ks3:

$$P = D(Ks3, Cpks3).$$

Then, the encrypted data Cmks2 is decrypted to use it by the decrypted copyright management program P and the decrypted second secret-key Ks2:

$$M = D(Ks2, Cmks2).$$

As described above, the third private-key Kv3 and the fourth private-key Kv4 are prepared by a secondary user but not opened to others. Therefore, even if a third party obtains the encrypted data Cmks2, it is impossible to use the data by decrypting it.

In the above described embodiment, the database 1, secondary copyright management center 14, tertiary copyright management center 15, and n-order copyright management center 16 are separately arranged in order to avoid the congestion of utilization requests. However, if the congestion of utilization requests does not matter, it is possible to combine all or some of these sections into one.

[Embodiment 5]

Figure 3 shows the system structure of embodiment 5. In embodiment 5, original data is encrypted and supplied one-way from a single database and a user selects necessary data out of the supplied original data to use it.

This embodiment uses a secret-key cryptosystem as its crypt key system.

In Figure 3, reference numberal 1 represents a database in which text data, binary data serving as computer graphics display or computer program, digital audio data, and digital picture data are stored by being encrypted, 2 represents a space satellite such as a communication satellite or a broadcasting satellite, 3 represents a data recording medium such as a CD-ROM or a flexible disk, 8 represents a communication network such as a pubilc telephone line offered y a communication enterprise or a CATV line offered by a cable television enterprise, and 4 represents a primary user terminal. And 17 represents a copyright management center for managing the copyright on data, and 5, 6, and 7 represent a secondary user terminal, tertiary user terminal, and n-order user terminal respectively.

On the above arrangement, the database 1, copyright management center 17, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6 and n-order user terminal 7 can be connected each other by the communication network 8.

Each user who uses this system is previously entered in the database system, and when entered in the system, database utilization software is given to him. This software includes a normal communication software program such as a data communication protocol.

Though the software for using the database system can be stored in a hard disk in a user terminal, it may be stored in a mask ROM, EPROM, or EEPROM built in the user terminal.

In this system, a secret-key generation algorithm is stored in a user terminal in order to generate a secret-key at the user side. However, because the secret-key generation algorithm is not always secret, it is also possible to store the algorithm in the database utilization software supplied to a user when he enters database utilization in the database system.

When original data is supplied free of charge because it is provided with advertisement, it may not be necessary to be encrypted. Even in this case, however, a procedure for using a copyright is necessary because the data is provided with a copyright.

In Figure 3, a route shown by a broken line represents a path of encrypted data, a route shown by a solid line represents a path requested from each user terminal, and a route shown by a one-dot chain line represents a path through which a crypt key corresponding to a utilization request is transferred.

The original data M0 stored in the database 1 or the data recording medium 3 is supplied to the primary user terminal 4 through a cable transmission via the communication network 8, by broadcast waves via the satellite 2 or the like, or by recording medium 3, and in this time, the data M0 is encrypted by the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0).$$

Similarly to the cases of embodiments 1 to 4, to protect the copyright of the original data Cm0ks1 which is encrypted to be supplied, when storing, copying, or transmitting which is utilization other than displaying or displaying for editing is applied to the original data M0 in the primary user terminal 4, the data is encrypted by the second secret-key Ks2:

$$Cm0ks2 = E(Ks2, M0)$$

as disclosed in Japanese Patent Application No. 64889/1994 which is the prior application by the inventor of the present invention et al. and, in the subsequent utilization, the original data is encrypted/decrypted by the second secret-key Ks2.

A primary user obtaining the encrypted original data Cm0ks1 designates an original data name or original data number from the primary user terminal 4 to request for the primary utilization of the encrypted original data Cm0ks1 to the copyright management center 17.

The copyright management center 17 receiving the primary utilization request of the encrypted original data Cm0ks1 from the primary user terminal 4 transfers the copyright management program P to the primary user terminal 4 together with the first secret-key Ks1.

The copyright management program P includes a crypt program having a cryptgraphic algorithm, which generates a secret-key and decrypts or encrypts data.

The primary user terminal 4 receiving the first secret-key Ks1 and the copyright management program P decrypts the encrypted original data Cm0ks1 by the first secret-key Ks1 using the crypt program

$$M0 = D(Ks1, Cm0ks1)$$

and uses the decrypted original data M0 directly or data M1 as edited.

The copyright management program P generates a second secret-key Ks2 in accordance with the first secret-key Ks1:

$$Ks2 = P(Ks1).$$

When the data M as the original data M0 or the edited data M1 is stored in the primary user terminal 4, copied to the recording medium 11, or transmitted to the secondary user terminal 5, the data is encrypted by the second secret-key Ks2 using the copyright management program P:

$$Cmks2 = E(Ks2, M).$$

The data Cmks2 encrypted by the second secret-key Ks2 is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8 together with the original data name or original data number.

The secondary user obtaining the encrypted data Cmks2 requests for the secondary utilization of the encrypted data Cmks2 to the copyright management center 17 from the secondary terminal 5 by designating the original data name or original data number.

The copyright management center 17 receiving the secondary utilization request of the encrypted data Cmks2 finds out the first secret-key Ks1 in accordance with the original data name or original data number, and generates the second secret-key Ks2 by the first secret-key Ks1 using the copyright management program P

$$Ks2 = P(Ks1),$$

and supplies the generated second secret-key Ks2 to the secondary user termina 15 together with the copyright management program P.

The secondary user terminal 5 receiving the second secret-key Ks2 and the copyright management program P decrypts the data Cmks2 encrypted by the second secret-key Ks2 by the second secret-key Ks2

$$M = D(Ks2, Cmks2)$$

and uses the data by displaying or editing it.

When the decrypted data M is stored in the secondary user terminal 5, stored in the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the copyright management program P.

Moreover, it is possible to make the copyright management program P generate the third secret-key Ks3 in accordance with the second secret-key Ks2:

$$Ks3 = P(Ks2),$$

so that the data M is encrypted by the third secret-key Ks3 using the copyright management program P when the data M is stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8:

$$Cmks3 = E(Ks3, M).$$

[Embodiment 6]

Then, embodiment 6 is described. Original data is encrypted and supplied one-way from a single database to a user and the user selects necessary data out of the original data to use it, similarly to the case of embodiment 5.

This embodiment uses a secret-key cryptosystem as its crypt key system anda second secret-key is generated in accordance with primary user information and a first secret-key.

Because the system structure of embodiment 6 is same to that of embodiment 5 shown in Figure 3, its description is omitted.

In the embodiment 6, the original data M0 stored in the database 1 is encrypted via the communication network 8, by broadcast waves via the satellite 2, or by the recording medium 3 using the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0)$$

and supplied to the primary user terminal 4.

A primary user obtaining the encrypted original data Cm0ks1 requests for primary utilization of the encrypted original data Cm0ks1 from the primary user terminal 4. In this time, the primary user must designate an original data name or original data number and present the primary user information Iu1.

The copyright management center 17 receiving the primary utilization request of the encrypted original data Cm0ks1 from the primary user supplies the first secret-key Ks1 and the copyright management program P to the primary user terminal 4.

The copyright management program P includes a crypt program having a cryptographic algorithm, which generates a secret-key and thus performs decryption and encryption.

The primary user terminal 4 receiving the first secret-key Ks1 and the copyright management program P decrypts the encrypted original data Cm0ks1 by the first secret-key Ks1 using the crypt program P

$$M0 = D(Ks1, Cm0ks1)$$

and uses the decrypted original data M0 directly or data M1 as edited.

The supplied copyright management program P generates the second secret-key Ks2 in accordance with the primary user information Iu1 or the primary user information Iu1 and the first secret-key Ks1:

$$Ks2 = P(Iu1) \text{ or}$$

$$Ks2\ P(Iu1 + Ks1).$$

Because the generated second secret-key Ks2 is based on the primary user information Iu1, it is impossible to generate the second secret-key Ks2 without the correct primary user information Iu1.

Furthermore, it is possible to use primary user data generated in accordance with the primary user information Iu1 or the terminal number of the primary user terminal 4 instead of the primary user information Iu1.

When the data M serving as the original data M0 or edited data M1 is stored in the primary user terminal 4, copied to the recording medium 11, or supplied to the secondary user terminal 5 via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the copyright management program P:

$$Cmks2 = E(Ks2, M).$$

The data Cmks2 encrypted by the second secret-key Ks2 is copied to the recording medium 11 or supplied to the secondary user terminal 5 via the communication network 8 together with its original data name or original data number and the primary user information Iu1.

A secondary user obtaining the encrypted data Cmks2 requests for secondary utilization of the data M to the copyright management center 17 from the secondary user terminal 5. In this time, the user must designate the original data name or original data number and present the primary user information Iu1.

The copyright management center 17 receiving the secondary utilization request of the data M finds out the first secret-key Ks1 in accordance with the original data name or original data number, generates the second secret-key Ks2 in accordance with either of the primary user information Iu1 and first secret-key Ks1, or both, and supplies the generated second secret-key Ks2 to the secondary user terminal 5 together with the copyright management program P.

The secondary user receiving the second secret-key Ks2 and the copyright management program P decrypts the encrypted data Cmks2 by the second secret-key Ks2 using the copyright management program P and in the secondary user terminal 5 to use it:

$$M = D(Ks2, Cmks2).$$

When the data M is stored in the secondary user terminal 5, copied to the recording medium 12, or supplied to the tertiary user terminal 6 via communication network 8, the data is encrypted by the second secret-key Ks2.

Moreover, it is possible to make the copyright management program P generate the third secret-key Ks3 in accordance with the second secret-key Ks2 using the copyrignt management program P:

$$Ks3 = P(Ks2)$$

so that the data M is encrypted by the third secret-key Ks3 when the data is stored in the secondary user terminal 5, copied to the recording medium 12, or supplied to the tertiary user terminal 6 via the communication network 8.

It is further possible to make the secondary user present the secondary information Iu2 when requesting for secondary utilization to the copyright management center 17 so that the third secret-key Ks3 is generated in accordance with the presented secondary user information Iu2 .

In this embodiment 6, if the copyright management program P for generating the second secret-key Ks2 can

be used in entire database system in common, the same second secret-key Ks2 is generated for the same original data in any database system as long as the primary user information Iu1 or the first secret-key Ks1 is not changed.

[Embodiment 7]

Then, embodiment 7 is described below. Original data is encrypted and supplied one-way to a user from a single database and the user selects necessary data out of the original data to use it similarly to the embodiments 5 and 6.

In this embodiment, a second secret-key is generated in accordance with the use frequency of a copyright management program and with a first secret-key.

This embodiment uses a secret-key cryptosystem.

Because the system structure of embodiment 7 is same to that of embodiments 5 and 6 shown in Figure 3, its description is omitted.

The original data M0 stored in the database 1 is encrypted by the first secret-key Ks1 via the communication network 8 or broadcast waves via the satellite 2, or by the recording medium 3:

$$Cm0ks1 = E(Ks1,M0),$$

and supplied to the primary user terminal 4.

A primary user obtaining the encrypted original data Cm0ks1 requests for primary utilization of the original data M0 to the copyright management center 17 from the primary user terminal 4 by designating an original data name or original data number.

The copyright management center 17 receiving the primary utilization request of the original data M0 transfers the first secret-key Ks1 and the copyright management program P to the primary user terminal 4.

The copyright management program P includes a crypt program having a cryptographic algorithm, in which a crypt key is generated and data is decrypted or encrypted.

Moreover, a counter is attached to the copyright management program P to count the use frequency of the program P.

The primary user receiving the first secret-key Ks1 and the copyright management program P decrypts the encrypted original data Cm0ks1 by the first secret-key Ks1 using the copyright management program P:

$$M0 = D(Ks1, Cm0ks1)$$

to use the decrypted original data M0 directly or data M1 as edited.

In the case of this system, when the data M serving as the original data M0 or edited data M1 is stored in the primary user terminal 4, copied to the recording medium 11, or transmitted to the secondary user terminal 5 via the communication network 8 in order to manage the copyright of data, the data is encrypted by the second secret-key Ks2 using the copyright management program P. The second secret-key Ks2 used for this operation is generated in accordance with the use frequency N of the copyright management program and with the first secret-key Ks1:

$$Ks2 = P(N + Ks1).$$

Because the second secret-key Ks2 thus generated is based on the use frequency N of the copyright management program P and the first secret-key Ks1, the data M is encrypted by the latest second secret-key Ks2 whenever it is used:

$$Cmks2 = E(Ks2, M).$$

The data Cmks2 encrypted by the second secret-key Ks2 generated through the final utilization is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8 together with its original data name or original data number and counter data N1.

The secondary user obtaining the encrypted data Cmks2 presents the original data name or original data number and the counter data N1 from the secondary user terminal 5 to request for the secondary utilization of the encrypted data Cmks2 to the copyright management center 17.

The copyright management center 17 receiving the secondary utilization request of the encrypted data Cmks2 finds out the first secret-key Ks1 in accordance with the presented original data name or original data number, generates the second secret-key Ks2 in accordance with the counter data N1 and the first secret-key Ks1, and supplies the second secret-key Ks2 to the secondary user terminal 5 together with the copyright management program P via the communication network 8.

The secondary user receiving the second secret-key Ks2 and the copyright management program P decrypts the encrypted data Cmks2 by the second secret-key Ks2 using the copyright management program P:

$$M = D(Ks2, Cmks2)$$

and uses the decrypted data M directly or by editing the data M.

When the data M is stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the copyright management program P:

$$Cmks2 = E(ks2, M).$$

In this case, it is also possible to make the copyright management program P generate the third secret-key Ks3 in accordance with a use frequency N2 of the copyright management program P in the secondary user terminal 5 and with the secret-key Ks2:

$$Ks3 = P(N2 + Ks2).$$

When the data M is stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user 6 via the communication network 8, the data M is encrypted by the third secret-key Ks3 using the copyright management program P:

$$Cmks3 = E(Ks3, M).$$

[Embodiment 8]

Figure 4 shows the system structure of embodiment 8 of the data copyright management system. In this embodiment, original data is supplied one-way to a user from a single database in accordance with a request of the user.

This embodiment uses a secret-key cryptosystem as its cryptosystem in which a second secret-key is generated in accordance with a first secret-key.

In Figure 4, reference numeral 1 represents a database, 4 represents a primary user terminal, 5 represents a secondary user terminal, 6 represents a tertiary user terminal, and 7 represents an n-order user terminal. And 18 represents a copyright management center and 8 represents a communication network such as a pubilc telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise.

In the above arrangement, the database 1, copyright management center 18, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-order user terminal 7 can be connected each other by the communication network 8.

Each user who uses this system must previously be entered in a database system, and when entered in the system, database system software is given to the user. This software includes a normal communication software such as a data communication protocol.

The database utilization software can be stored in a hard disk of a user terminal, and may be stored in a mask ROM, EPROM, or EEPROM built in the user terminal.

In this system, a secret-key generation algorithm is stored in a user terminal in order to generate a secret-key at the user side. However, because the secret-key generation algorithm is not always secret, it is possible to store the algorithm in the database uatilization software given to the user when the user is entered in a database system.

In case of original data provided with advertisement supplied to the user free of charge, it may not be necessary to encrypt the data. Even in this case, however, because the data has a copyright, a procedure for using the copyright is necessary.

In Figure 4, a route shown by a broken line represents a path for encrypted data, a route shown by a solid line represents a path requested from each user terminal, and a route shown by a one-dot chain line represents a path through which a key for allowing data utilization and a copyright management program together with a secret-key from the copyright management center to secondary and subsequent-order user.

In Figure 4, the database 1 stores text data, graphics data or binary data, audio data, and picture data which are not encrypted.

A primary user requests for utilization of the original data M0 from the primary user terminal 4 by designating an original data name or number to the database 1 via the communication network 8.

The database 1 receiving the utilization request of the original data M0 from the primary user terminal 4 encrypts the original data M0 by the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0)$$

and supplies the copyright management program P to the primary user terminal 4 together with the encrypted original data Cm0ks1 and the first secret-key Ks1.

The copyright management program P includes a crypt program having a cryptographic algorithm which generates a secret-key and decrypts or encrypts data.

Moreover, by making the cryptographic algorithm depend on the first secret-key Ks1, it is possible to make the copyright management program P inherent in the original data M0.

The primary user terminal 4 receiving the first secret-key Ks1 and the copyright management program P together with the original data Cm0ks1 encrypted by the first secret-key Ks1 decrypts the encrypted original data Cm0ks1 by the first secret-key Ks1:

$$M0 = D(Ks1, Cm0ks1),$$

and uses the decrypted original data M0 directly or data M1 as edited.

And the copyright management program P generates the second secret-key Ks2 in accordance with the first secret-key Ks1:

$$Ks2 = P(Ks1).$$

When the data M as decrypted original data or edited data is stored in the primary user terminal 4, copied to the recording medium 11, or transmitted to the secondary user terminal 5 via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the copyright management program P:

$$Cmks2 = E(Ks2, M).$$

The encrypted data Cmks2 is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8, together with its original data name or original data number.

A secondary user obtaining the encrypted data Cmks2 requests for secondary utilization of the data M as original data or edited data to the copyright management center 18 from the secondary user terminal 5 by designating the original data name or number.

The secondary copyright management center 18 receiving the secondary utilization request of the data M finds out the first secret-key Ks1 in accordance with the original data name or original data number to generate the second secret-key Ks2 in accordance with the first secret-key Ks1:

$$Ks2 = P(Ks1),$$

and supplies the generated second secret-key Ks2 to the secondary user terminal 5 together with the copyright management program P.

The secondary user terminal 5 receiving the second secret-key Ks2 and the copyright management program P decrypts the encrypted data Cmks2 by the second secret-key Ks2 using the copyright management program P:

$$M = D(Ks2, Cmks2)$$

and uses the decrypted data M directly or by editing it.

When the data M is stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8.

A third secret-key Ks3 is generated by the copyright management program P in accordance with the second secret-key Ks2:

$$Ks3 = P(Ks2)$$

so that the data M is encrypted by the generated third secret-key Ks3 using the copyright management program P:

$$Cmks3 = E(Ks3, M).$$

[Embodiment 9]

In the case of embodiment 9 described below, original data is supplied to a user from a single database in accordance with a request of the user, similarly to embodiment 8 in Figure 4.

This embodiment uses a secret-key cryptosystem and user data in addition to the first secret-key used for embodiment 8 to generate a second secret-key.

Because the system structure of this embodiment is same to that of embodiment 8, its description is omitted.

The database 1 stores the original data M0 which is not encrypted.

When a primary user accesses the database 1 from the primary user terminal 4, a data menu is transferred to the user. In this case, it is possible to display charge information together with the data menu.

When the primary user receives the data menu, the user retrieves the data menu to select the original data M0 and requests for primary utilization of the original data M0 to the database 1 by designating the original data name or the like of the selected original data M0.

In the database 1 receiving the utilization request of the original data M0 from the primary user terminal 4, the original data M0 is read and the read original data M0 is encrypted by the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0)$$

and the copyright management program P is supplied to the primary user terminal 4 together with the encrypted original data Cm0ks1 and the first secret-key Ks1.

The copyright management program P used here is common to entire database system, which includes a crypt program having a cryptographic algorithm. A crypt key is generated and data is decrypted or encrypted by this crypt program.

The primary user terminal 4 receiving the first secret-key Ks1 and the copyright management program P decrypts the encrypted original data Cm0ks1 by the first secret-key Ks1 using the copyright management program P:

$$M0 = D(Ks1, Cm0ks1)$$

and uses the decrypted original data M0 directly or data M1 as edited.

The copyright management program P generates the second secret-key Ks2 in accordance with a primary user information Iu1:

$$Ks2 = P(Iu1).$$

The second secret-key Ks2 may be generated in accordance with the first secret-key Ks1 or the primary user data Iu1 and the first secret-key Ks1 instead of the primary user information Iu1:

$$Ks2 = P(Ks1)$$

$$Ks2 = P(Ks1 + Iu1).$$

When the data M serving as the original data M0 or edited data M1 is stored in the primary user terminal 4, copied to the recording medium 11, or transmitted to the secondary user terminal 5 via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the copyright management program P:

$$Cmks2 = E(Ks2, M).$$

The data Cmks2 encrypted by the second secret-key Ks2 is provided with the original data name or original data number and then, copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8.

A secondary user obtaining the data Cmks2 encrypted by the second secret-key Ks2 requests for secondary utilization of the data M to the copyright management center 18 from the secondary user terminal 5. In this time, the user designates the original data name

or original data number and presents the uncrypted primary user information Iu1.

The copyright management center 18 receiving the secondary utilization request of the data M finds out the first secret-key Ks1 in accordance with the designated original data name or original data number, generates the second secret-key Ks2 in accordance with the presented primary user information Iu1 and the found-out first secret-key Ks1 by the copyright management program P, and supplies the key Ks2 to the secondary user terminal 5 together with the copyright management program P.

The secondary user obtaining the second secret-key Ks2 and the copyright management program P decrypts the encrypted data Cmks2 by the second secret-key Ks2 using the copyright management program P in the secondary user terminal 5:

$$M = D(Ks2, Cmks2)$$

and uses the decrypted data M directly or by editing the data.

When the data M is stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the copyright management program P:

$$Cmks2 = E(Ks2, M).$$

In this case, it is also possible to make the copyright management program P generate the third secret-key Ks3 in accordance with the primary user information Iu1, second secret-key Ks2, or primary user information Iu1 and the second secret-key Ks2,

$$Ks3 = P(Iu1)$$

$$Ks3 = P(Iu1+Ks1)$$

$$Ks3 = P(Ks1).$$

It is also possible to make the secondary user present the secondary user information Iu2 when requesting for secondary utilization so that the third secret-key is generated in accordance with the secondary user information Iu2 instead of the primary user information Iu1.

The data M is encrypted by the third secret-key Ks3 using the copyright management program P:

$$Cmks = E(Ks3, M).$$

In this embodiment, the copyright management program P for generating the second secret-key Ks2 is common to any database. Therefore, in any database, the same second secret-key Ks2 is generated for the same original data as long as the primary user data Iu1 and the first secret-key Ks1 are not changed.

[Embodiment 10]

In the case of embodiment 10 described below, original data is supplied to a user from a single database in accordance with a request of the user similarly to the case of embodiment 8.

This embodiment uses a secret-key cryptosystem.

This embodiment uses the use frequency of a copyright management program instead of user information adopted for generating a second secret-key in embodiment 9.

Because the system structure of this embodiment is same to that of embodiment 8, its description is omitted.

The database 1 stores original data M0 which is not encrypted.

When a primary user accesses the database 1 from the primary user terminal 4, a data menu is transferred to the user. In this time, charge information may be displayed together with the data menu.

When the primary user receives the data menu, the user retrieves the data menu to select the original data M0 and requests for the primary utilization of the original data M0 to the database 1 by designating an original data name or the like via communication network 8 from the primary user terminal 4.

The database 1 receiving the data utilization request from a primary user encrypts the original data M0 by a first secret-key Ks1

$$Cm0ks1 = E(Ks1, M0)$$

and supplies the copyright management program P to the primary user terminal 4 together with the encrypted data Cm0ks1 and the first secret-key Ks1.

The copyright management program P includes a crypt program having a cryptographic algorithm, which generates a crypt key and decrypts or encrypts data.

Moreover, a counter is attached to the copyright management program P to count the use frequency N of the program P or the number of use times of original data.

Furthermore, by making the cryptographic algorithm depend on the first secret-key Ks1, it is possible to make the copyright management program P inherent in the original data.

The primary user receiving the first secret-key Ks1 and the copyright management program P decrypts the encrypted original data Cm0ks1 by the first secret-key Ks1 using the copyright management program P

$$M0 = D(Ks1, Cm0ks1)$$

and uses the decrypted original data M0 directly or data M1 as edited.

To protect the copyright of data, when the data M as the original data M0 or edited data M1 is stored in the primary user terminal 4, copied to the recording medium

11, or transmitted to the secondary user terminal 5 via the communication network 8, the data M is encrypted by the copyright management program P. In other words, a copyright management program always runs whenever these types of utilization are performed.

When the supplied copyright management program P is used, the counter in the program performs counting and the copyright management program P generates the second secret-key Ks2 in accordance with the counted value N and the first secret-key Ks1:

$$Ks2 = P(N + Ks2).$$

Because the second secret-key Ks2 is based on the use frequency N of the copyright management program P, the data M is encrypted by the new second secret - key Ks2 whenever the data is used:

$$Cmks2 = E(Ks2, M).$$

The data Cmks2 encrypted by the finally generated second secret-key Ks2 is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8 together with the original data name or original data number, the primary user information Iu1 and the counter data N.

A secondary user obtaining the data Cmks2 encrypted by the second secret-key Ks2 presents the original data name or original data number, primary user information Iu1, and counter data N to request for secondary utilization of the data M to the copyright management center 18.

The copyright management center 18 receiving the secondary utilization request of the encrypted data Cmks2 finds out the first secret-key Ks1 in accordance with the original data name or original data number of the data, generates a second secret-key Ks2 according to the first secret-key Ks1, and the presented primary user information Iu1 and the counter data N, and transfers the generated second secret-key Ks2 to the secondary user terminal 5 together with the copyright management program P.

The secondary user terminal 5 receiving the second secret-key Ks2 and the copyright management program P decrypts the encrypted data Cmks2 by the second secret-key Ks2 using the copyright management program P

$$M = D(Ks2, Cmks2)$$

and uses the decrypted data M directly or by editing the data.

When the data is stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8, the data is encrypted by the second secret-key using the copyright management program P.

Moreover, it is possible that the copyright management program generates a third secret-key in accordance with the second secret-key.

Above-mentioned embodiments 1 to 10 are described about a case of using a single original data supplied from a database. However, one of the data utilization, editing includes not only a case of editing a single data but also a case of producing new data by combining a plurality of original data obtained from the same database and a case of producing new data by combining a plurality of original data obtained from a plurality of databases.

[Embodiment 11]

Embodiment 11 to be described below is an embodiment in which a primary user produces new data by combining a plurality of original data stored in a single database. That is, the primary user produces new data by using first, second, and third original data stored in the database.

In this embodiment, a plurality of original data are supplied to a user from a single database in response to a request of the user similarly to the case of embodiment 8 shown in Figure 4.

This embodiment uses a secret-key cryptosystem.

Because the system structure of this embodiment is same to that of embodiment 8, its description is omitted.

The database 1 stores original data M01, M02 and M03 which are not encrypted.

When the primary user accesses the database 1 from the primary user terminal 4, a data menu is transferred to the user. In this time, charge information may be displayed together with the data menu.

When the primary user receives the data menu, the user retrieves the data menu to select the original data M01, M02 and M03 and requests for supply of the data M01, M02 and M03 to the database 1 via the communication network 8 by designating original data names or original data numbers of the first, second and third original data M01, M02 and M03, and also presents the primary user information Iu1.

The database 1 receiving the supply request of the first, second and third original data M01, M02 and M03 from the primary user encrypts the first, second and third original data M01, M02 and M03 by first, second and third secret-keys Ks01, Ks02 and Ks03 respectively:

$$Cm01ks01 = E(Ks01, M01)$$

$$Cm02ks02 = E(Ks02, M02)$$

$$Cm03ks03 = E(Ks03, M03)$$

and supplies the first, second and third secret-keys Ks01, Ks02 and Ks03 and the copyright management program P common to entire database and all original data to the primary user terminal 4.

The copyright management program P incudes a crypt program having a cryptographic algorithm, which generates a crypt key and decrypts or encrypts data.

The primary user terminal 4 receiving the first encrypted original data Cm01ks01, second encrypted original data Cm02ks02, third encrypted original data Cm03ks03, first secret-key Ks01, second secret-key Ks02, third secret-key Ks03, and copyright management program P decrypts the first, second and third encrypted original data Cm01ks01, Cm02ks02 and Cm03ks03 by the secret-keys Ks01, Ks02, and Ks03 using the copyright management program P

$$M01 = D(Ks01, Cm01ks01)$$

$$M02 = D(Ks02, Cm02ks02)$$

$$M03 = D(Ks03, Cm03ks03),$$

and produces new data M1 edited from the original data M01, M02 and M03.

The copyright management program P produces a fourth secret-key Ks4 in accordance with one or some of the first secret-key Ks01, second secret-key Ks2, third secret-key Ks3, and primary user data lu1:

$$Ks4 = P(Ks01/Ks02/Ks03/lu1).$$

When the edited data M1 is stored in the primary user terminal 4, copied to the recording medium 11, or transmitted to the secondary user terminal 5 via the communication network 8, the data is encrypted by the fourth secret-key Ks4 using the copyright management program P:

$$Cm1ks4 = E(Ks4, M1).$$

The encrypted edited data Cm1ks4 is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8, together with original data names or original data numbers and the primary user data lu1.

A secondary user obtaining the encrypted edited data Cm1ks4 requests for secondary utilization of the data Cm1ks4 to the copyright management center 18 from the secondary user terminal 5. In this time, the user designates data names or data numbers of the original data M01, M02 and M03 and presents the primary user information lu1.

The copyright management center 18 receiving the secondary utilization request of the encrypted edited data Cm1ks4 from the secondary user finds out the first secret-key Ks01 in accordance with the data name or data number of the first original data M01, the second secret-key Ks02 in accordance with the data name or number of the second original data M02, and the third secret-key Ks03 in accordance with the data name or number of the third original data M03; generates fourth secret-key Ks4 by one or some of the found-out first secret-key Ks01, second secret-key Ks02, third secret-key Ks03 and primary user information lu1 using common copyright management program P

$$Ks4 = P(Ks01/Ks02/Ks03/lu1);$$

and supplies the fourth secret-key Ks4 to the secondary user terminal 5 together with the common copyright management program P.

The secondary user receiving the fourth secret-key Ks4 and the common copyright management program P decrypts the encrypted edited data Cm1ks4 by the fourth secret-key Ks4 using the copyright management program P

$$M1 = D(Ks4, Cm1ks4)$$

and uses the decrypted edited data M1 directly or data M2 as edited.

When the edited data M1 or re-edited data M2 is stored in the secondary user terminal 5, copied to the recording medium 12 or transmitted to a tertiary user terminal 6 via the communication network 8, a fifth secret-key Ks5 is generated in accordance with the fourth secret-key Ks4 by the copyright management program P, and the data is encrypted by the fifth secret-key Ks5 using the copyright management program P:

$$Cm1ks5 = E(Ks5, Cm1)$$

$$Cm2ks5 = E(Ks5, Cm2).$$

Moreover, it is possible to make the common copyright management program P generate a fifth secret-key Ks5 by the fourth secret-key Ks4 for subsequent encryption or decryption by the generated fifth secret-key Ks5.

In this embodiment, a copyright management program for generating a fourth secret-key is common to any database. Therefore, in any database, the same fourth secret-key is generated for the same original data as long as primary user data and a first secret-key are not changed.

While the common copyright management program of this embodiment is supplied from the copyright management center 18, it may be stored in a ROM in each user terminal or in software for using a database.

[Embodiment 12]

Embodiment 12 described below is an embodiment in which new data is produceed by combining a plurality of original data supplied from a plurality of databases in response to a user's request. This embodiment uses a secret-key cryptosystem.

In Figure 5, reference numerals 19, 20, and 21 represent first, second and third databases storing text data, binary data as a computer graphics display or computer program, and audio data or picture data, 4 represents a primary user terminal, 5 represents a secondary user

terminal, 6 represents a tertiary user terminal, 7 represents an n-order user terminal, 10 represents a copyright management center for managing data copyrights, and 8 represents a communication network such as a public telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise.

In the above arrangement, the first, second and third databases 19, 20 and 21, copyright management center 10, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-order user terminal 7 can be connected each other by the communication network 8.

Each user who desires to use this system must previously be entered in each database system, and when entered in the database system, database utilization software is supplied to the user. The software includes a normal communication software program such as a data communication protocol.

The database utilization software can be stored in a hard disk of a user terminal, and also may be stored in a mask ROM, EPROM, or EEPROM built in the user terminal.

In this system, a crypt key generation algorithm is stored in a user terminal in order to generate a secret-key at the user side. However, because the crypt key generation algorithm is not necessarily secret, it is possible to store the algorithm in each database utilization software.

In case of original data provided with advertisement supplied to the user free of charge, it may not be necessary to encrypt the data. Even in this case, however, because the data has a copyright, a procedure for using the copyright is necessary.

In this drawing, a route shown by a broken line represents a path for encrypted data, a route shown by a solid line represents a path of requests from each user terminal to each database and copyright management center, and route shown by a one-dot chain line represents a path through which permit information corresponding to utilization requests, a copyright management program, and a crypt key are transferred from each database and copyright management center to each user terminal.

This embodiment uses a secret-key and a copyright management program which are different for each original data and are previously stored in each database and the copyright management center.

The first database 19 stores the first original data M1 which is not encrypted. When a primary user accesses the first database 19 from the first user terminal 4, a data menu is transferred to the user.

When the primary user receives the data menu, the user retrieves the data menu to select the first original data M1 and requests for supply of the first original data M1 to the first database 19 via the communication network 8 from the primary user terminal 4 by designating an original data name or original data number. In this time, the user presents the primary user information Iu1.

The first database 19 receiving the utilization request of the first original data M1 from the primary user encrypts the requested first original data M1 by first secret-key Ks1

$$Cm1ks1 = E(Ks1, M1)$$

and supplies the encrypted data to the primary user terminal 4.

The second database 20 stores the second original data M2 which is not encrypted. When the primary user accesses the second database 20 from the primary user terminal 4, a data menu is transferred to the user.

When the primary user receives the data menu, the user retrieves the data menu to select the second original data M2 and requests for supply of the second original data M2 to the second database 20 via the communication network 8 from the primary user terminal 4 by designating an original data name or original data number. In this time, the user presents the primary user information Iu1.

The second database 20 receiving the utilization request of the second original data M2 from the primary user encrypts the requested second original data M2 by second secret-key Ks2

$$Cm2ks2 = E(Ks2, M2)$$

and supplies the encrypted data to the primary user terminal 4.

The third database 21 stores the third original data M3 which is not encrypted. When the primary user accesses the third database 21 from the primary user terminal 4, a data menu is transferred to the user.

When the primary user receives the data menu, the user retrieves the data menu to select the third original data M3 and requests for supply of the third original data M3 to the third database 21 via the communication network 8 from the primary user terminal 4 by designating an original data name or original data number. In this time, the user presents the primary user information Iu1.

The third database 21 receiving the utilization request of the third original data M3 from the primary user encrypts the requested third original data M3 by the third secret-key Ks3

$$Cm3ks3 = E(ks3, M3)$$

and supplies the encrypted data to the primary user terminal 4.

The primary user receiving the first, second, and third encrypted original data Cm1ks1, Cm2ks2 and Cm3ks3 requests for primary utilization of the first, second, and third encrypted original data Cm1ks1, Cm2ks2 and Cm3ks3 to the copyright management center 10 via the communication network 8 from the primary user terminal 4 by designating original data names or numbers.

The copyright management center 10 receiving the primary utilization request of the first, second and third

encrypted original data Cm1ks1, Cm2ks2 and Cm3ks3 from the primary user supplies a first copyright management program P1, a second copyright management program P2, and a third copyright management program P3 to the primary user terminal 4 together with the first secret-key Ks1 as a crypt key of the first original data M1, the second secret-key Ks2 as a crypt key of the second original data M2, and the third secret-key Ks3 as a crypt key of the third original data M3.

These copyright management programs P1, P2 and P3 include a crypt program having a cryptographic algorithm respectively, which generates new secret-keys and decrypts or encrypts data.

Moreover, by making these cryptographic algorithms depend on the first, second and third secret-keys Ks1, Ks2 and Ks3 respectively, it is possible to make the first, second and third copyright management programs P1, P2 and P3 inherent in the first, second and third original data M1, M2 and M3 respectively.

The primary user terminal 4 receiving the first, second and third secret-keys Ks1, Ks2 and Ks3 decrypts the first, second and third original data Cm1ks1, Cm2ks2 and Cm3ks3 encrypted by these secret-keys:

$$M1 = D(Ks1, Cm1ks1)$$

$$M2 = D(Ks2, Cm2ks2)$$

$$M3 = D(Ks3, Cm3ks3),$$

and uses the decrypted original data M1, M2, and M3 directly or by editing them.

And the first copyright management program P1 generates fourth secret-key Ks4 in accordance with the first secret-key Ks1, the second copyright management program P2 generates fifth secret-key Ks5 in accordance with the second secret-key Ks2, and the third copyright management program P3 generates sixth secret-key Ks6 in accordance with the third secret-key Ks3:

$$Ks4 = P1(Ks1)$$

$$Ks5 = P2(Ks2)$$

$$Ks6 = P3(Ks3).$$

When the original data M1, M2 and M3 or edited data M4, M5 and M6 are stored in the primary user terminal 4, copied to the recording medium 11, or transmitted to the secondary user terminal 5 via the communication network 8; the first original data M1 or edited data M4 is encrypted by the fourth secret-key Ks4 using the first copyright management program P1, the second original data M2 or edited data M5 is encrypted by the fifth secret-key Ks5 using the second copyright-management program P2, and the third original data M3 or edited data M6 is encrypted by the sixth secret-key Ks6 using the third copyright management program P3:

$$Cm1ks4 = E(Ks4, M1)$$

$$Cm2ks5 = E(Ks5, M2)$$

$$Cm3ks6 = E(Ks6, M3)$$

$$Cm4ks4 = E(Ks4, M4)$$

$$Cm5ks5 = E(Ks5, M5)$$

$$Cm6ks6 = E(Ks6, M6).$$

The original data Cm1ks4, Cm2ks5 and Cm3ks6 or edited data Cm4ks4, Cm5ks5 and Cm6ks6 encrypted by the fourth, fifth and sixth secret-keys Ks4, Ks5 and Ks6 are copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 8 together with the first, second and third original data names or original data numbers and the primary user data Iu1.

For the secondary user terminal 5 receiving the first, second and third encrypted original data Cm1ks4, Cm2ks5 and Cm3ks6 or the encrypted edited data Cm4ks4, Cm5ks5 and Cm6ks6, secondary utilization of the first, second and third original data M1, M2 and M3 or edited data M4, M5 and M6 is requested to the copyright management center 10 by designating the original data names or original data numbers.

The copyright management center 10 receiving the secondary utilization request of the first, second and third original data M1, M2 and M3 or the edited data M4, M5 and M6 from the secondary user terminal 5 finds out the first secret -key Ks1 and the first copyright management program P1 in accordance with the first original data name or number, the second secret-key Ks2 and the second copyright management program P2 in accordance with the second original data name or number and the third secret-key Ks3 and the third copyright management program P3 in accordance with the third original data name or number; in which the first copyright management program P1 generates the fourth secret-key Ks4 from the first secret-key Ks1, the second copyright management program P2 generates the fifth secret-key Ks5 from the second secret-key Ks2 and the third copyright management program P3 generates the sixth secret-key Ks6 from the third secret-key Ks3

$$Ks4 = P1(Ks1)$$

$$Ks5 = P2(Ks2)$$

$$Ks6 = P3(Ks3);$$

and supplies these secret-keys to the secondary user terminal 5 together with the first, second and third copyright management programs P1, P2 and P3.

In the secondary user terminal 5 receiving the fourth, fifth and sixth secret-keys Ks4, Ks5 and Ks6 and the first, second and third copyright management programs P1,

P2 and P3, the encrypted first original data Cm1ks4 or edited data Cm4ks4 is decrypted by the fourth secret-key Ks4 using the first copyright management program P1, the encrypted second original data Cm2ks5 or edited data Cm5ks5 is decrypted by the fifth secret-key Ks5 using the second copyright management program P2, and the encrypted third original data Cm3ks6 or edited data Cm6ks6 is decrypted by the sixth secret-key Ks6 using the third copyright management program P3

$$M4 = D(Ks4, Cmks4)$$

$$M5 = D(Ks5, Cm5ks5)$$

$$M6 = D(Ks6, Cm6ks6),$$

and the decrypted data M4, M5 and M6 are used directly or by editing them.

When the first, second and third original data M1, M2 and M3 or edited data M4, M5 and M6 are stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8, the first original data M1 or edited data M4 is encrypted by the fourth secret-key Ks4 using the first copyright management program P1, the second original data M02 or edited data M5 is encrypted by the fifth secret-key Ks5 using the second copyright management program P2, and the third original data M3or edited data M6 is encrypted by the sixth secret-key Ks6 using the third copyright management program P3.

In this case, it is also possible to make the first copyright management program P1 generate a seventh secret-key Ks7 in accordance with the fourth secret-key Ks4, the second copyright management program P2 generate an eighth secret-key Ks8 in accordance with the fifth secret-key Ks5 and the third copyright management program P3 generate a ninth secret-key Ks9 in accordance with the sixth secret-key Ks6:

$$Ks7 = P1(Ks4)$$

$$Ks8 = P2(Ks5)$$

$$Ks9 = P3(Ks6)$$

and when the first, second and third original data M1, M2 and M3 or edited data M4, M5 and M6 are stored in the secondary user terminal 5, copied to the recording medium 12, or transmitted to the tertiary user terminal 6 via the communication network 8, the first, second and third copyright management programs P1, P2 and P3 encrypt the first, second and third original data M1, M2 and M3 or the edited data M4, M5 and M6 by the seventh, eighth and ninth secret-keys Ks7, Ks8 and Ks9:

$$Cm1ks7 = E(Ks7, M1)$$

$$Cm2ks8 = E(Ks9, M2)$$

$$Cm3ks9 = E(Ks9, M3)$$

$$Cm4ks7 = E(Ks7, M4)$$

$$Cm5ks8 = E(Ks8, M5)$$

$$Cm6ks9 = E(Ks9, M6)$$

[Embodiment 13]

Embodiment 13 described below is an embodiment in which new data is produced by using a plurality of original data supplied from a plurality of data bases in response to a user's request similarly to embodiment 12. This embodiment uses a secret-key cryptosystem.

The use frequency of copyright management programs is further used to generate a crypt key for encryption/decryption similarly to the cases of embodiments 7 and 11.

In this embodiment, a counter is attached to a copyright management program, which counts the service frequency of the program or the number of times of using original data and the fourth, fifth and sixth secret-keys Ks4, Ks5 and Ks6 are generated by the counter value N.

A secondary user presents the counter value N together with the original data name or original data number of each original data and primary user data to request for secondary utilization of data to the copyright management center 10.

The copyright management center 10 receiving the secondary utilization request of data finds out the first, second and third secret-keys Ks1, Ks2 and Ks3 in accordance with the original data names or original data numbers, generates fourth, fifth and sixth secret-keys Ks4, Ks5 and Ks6 by the first, second and third secret-keys Ks1, Ks2 and Ks3 for each data, the primary user information Iu1 and the first, second and third counter values N1, N2 and N3 using the first, second and third copyright management programs P1, P2 and P3; and supplies the generated fourth, fifth and sixth secret-keys Ks4, Ks5 and Ks6 to secondary user together with the fourth, fifth and sixth copyright management programs P1, P2 and P3.

Because the system structure of embodiment 13 is same to that of embodiment 12 except the above point, its detailed description is omitted.

[Embodiment 14]

When a copy of original data obtained by a primary user is directly supplied to a secondary user, a copyright of the primary user is not effected on the data because the data is not provided with any value. However, when new data is produced from obtained original data, that is, when new data is produced from obtained single original data or from a plurality of obtained original data, a secondary copyright of the primary user; i.e., secondary exploitation right in editing the data is effected on the new data.

Because the copyright of the original copyright owner also exists in the original data used for editing data, the original copyright of the original data of an author and the secondary copyright of the primary user who has edited data exist in the edited data.

As a copyright is not a mere real right but a right having essential element of a personal right, authors strongly insist on the existence of the copyright in many cases. Therefore, even when original data is edited, it is preferable that the original data or its copyright owner can easily be specified from the edited data.

In the data copyright management systems described in embodiments 1 to 13, the copyrights of data are managed by encrypting original data or edited data. For these systems, however, the copyright of data is managed without identifying] original data or edited data, in the whole data or separating an original data part from an edited data part in the whole edited data. Therefore, it is impossible to specify original data or owner out of edited data.

In embodiment 14 described below makes it possible to separate original data in which only the original copyright exists from edited data in which a secondary exploitation right also exists in addition to the original copyright, and moreover clearly manage the original copyright and the secondary exploitation right.

Because data is edited by using a program for edition and thereby altering original data, edited data can be reproduced as the original data and edit contents (further, the program for edition when necessary) are specified. In other words, unless the original data and the edit contents (further, the program for edition when necessary) are specified, it is impossible to reproduce the edited data.

In embodiment 14, the secondary exploitation right described is managed by specifying original data and edit contents (further, a program for edition when necessary) and managing them.

To produce new data from single original data, there are a case in which edited data [A'] is obtained by altering original data A, a case in which edited data [A+X] is obtained by adding data X to the original data A by a primary user;
a case in which edited data [A"] is obtained by dividing the original data A into original data elements A1, A2, A3,... and changing the arrangement of the elements to such as A3, A2 and A1; and a case in which edited data [A1+X1+A2+X2+ A3+X3...] is obtained by dividing the original data A into original data elements A1, A2, A3,....., also dividing the data X of the primary user into X1, X2, X3,... and arranging these elements.

In these cases, alteration of original data, change of original data arrangement, combination of the original data with primary user data, and division of the original data and combination of it with the primary user data can respectively be provided with a secondary exploitaion right, which is necessary to be protected. The original copyright of the primary user, of course, exists in the data X added by the primary user.

To produce new data by combining a plurality of original data, there are a case in which edited data [A+B+C...] is obtained by simply combining original data A, B, C,...; a case in which edited data such as [A+X] is obtained by adding data X to the original data A, B, C, ..., a case in which edited data [A1 +B1+C1+...+A2+B2+C2+...+A3+B3+C3+...] is obtained by dividing the original data A, B, C,... into original data elements A1, A2, A3,..., B1, B2, B3,..., and C1, C2, C3,..., combining them, and changing their arrangements; and a case in which edited data [A1+B1+C1+X1+...+A2+B2+C2+X2+...+A3+B3+C3+X3 +...] is obtained by dividing the original data A, B, C,... into original data elements A1, A2, A3,..., B1, B2, B3,..., and C1, C2, C3,..., combining the elements with primary user data X1, X2, X3,..., and changing their arrangements.

Also in these cases, combination of a plurality of original data, combination of a plurality of original data with primary user data, division of a plurality of original data and change of the arrangements, and combination of a plurality of divided original data with the primary user data can respectively be provided with a secondary exploitation right, which is necessary to be protected. Also, the original copyright of the primary user, of course, exists in the data X1, X2, X3,... added by the primary user.

Figure 6 shows an example for producing new data D by using a plurality of original data A, B and C. This method is known as the cut-and-paste technique in which data is edited by extracting (cutting out) elements "a", "b" and "c" from original data A, B and C and attaching (pasting) the extracted elements "a", "b" and "c" to form a piece of data D.

While it is clear that original data and primary user data are data, the editing process: alteration of original data, arrangement change of original data, combination of original data with primary user data, division of original data and combination with primary user data, combination of a plurality of original data each other, combination of a plurality of original data with primary user data, division and arrangement change of a plurality of original data, and combination of a plurality of divided original data with primary user data, are also data.

In the above described embodiments 1 to 13, the copyright of data are managed by encrypting original data or edited data. Moreover, when noticing that editing process of data, such as arrangement of original data and process of editing, is also data, the secondary exploitation right on edited data can be protected by managing the primary copyright of the author on the original data and secondary copyright of the primary user about editing process data.

Editing process data or program for edition may be called as scenario.

That is, it is possible to ensure to manage the copyrights of edited data as well as of original data, if the edited data is constituted with original data, primary user data and editing process data, and thus, these original

data, primary user data and editing process data are managed by the data copyright management system described in embodiments 1 to 13.

In this case, a program for edition used for editng data may be managed by the data copyright management system, if necessary.

While the above data edition of original data can be performed by using a program for edition corresponding to the original data, by handling the original data as object-oriented software which has recently been focused on, it is possible to facilitate further editing of data and manage more preferably copyrights of data.

Moreover, by adopting agent-oriented software, a user can synthesize data with little labor.

The agent-oriented software, unlike the conventional one, is a program having autonomy, flexibility and cooperativeness, which is able to meet a user's request with its characteristics of autonomy, flexibility and cooperativeness in accordance with only a general instruction of the user without specifically giving every operation instruction to the software.

By incorporating the agent program into a basic system of a data copyright management system so that the program monitors the database utilization of a user and information obtained through the monitoring is collected at the database or the copyright management center, it is possible to know the database utilization condition of the user at the database side or the copyright management center side and achieve more accurate copyright management.

As described, these agent program and data can also be protected and, therefore, are encrypted like original data.

[Embodiment 15]

Works include those with no copyright and those with a copyright and the works with a copyright include those which make use of the copyright and those which do not make use of the copyright.

The works with no copyright include those to which no copyright is given by a law and those whose copyright duration has passed. All works except those which have no existing copyright have a copyright, and they are normally provided with a mark for insisting on the copyright which prevents infringement of the copyright.

The same is applied to data as a work. In case of data with a copyright, indication of a copyright or an author mark is given to the data to be used or to the file header of the data in order to prevent the infringement of the copyright.

Further, by adding the copyright flag indicative of the data with copyright to the file, and by identifying the copyright flag in the user terminal, it is possible to prevent the infringement of the data copyright.

However, even if the indication on a copyright is given to data, when a user disregards the copyright of the data work that results in the infringement of the copyright.

To prevent the above case, in the above mentioned embodiments, data is encrypted and a decryption key for decrypting the encrypted data is managed so as to perform encryption or decryption by a crypt key different from the decryption key when decrypted data is stored, copied, or transmitted.

Even in this case, there may be the possibility of storing, copying, or transferring data without using a cryptographic key different from a decryption key by transmitting the data to a memory other than the main memory of a user terminal while the data is present in the main memory of the user terminal.

To prevent the above case, it is the best to incorporate data copyright utilization software into a basic system of a user terminal, indicate the file of a data work to which a copyright is given with an attribute for making use of the copyright, make the basic system of the user terminal monitor the attribute for using the copyright of the data work, and make the data copyright utilization software manage the data work having the copyright using attribute.

For the basic system means a software operating system such as DOS when the user terminal is a computer such as a personal computer or a hardware operating system stored in a ROM when the user terminal is a portable information terminal or STB (set top box).

To more completely manage a data copyright with the operating system, it is preferable to incorporate the data copyright utilization software into a higher-level operating system.

Every processing and every data in the user terminal is under control of an operating system. In other words, the operating system can hold every processing and data in the user terminal.

Therefore, it is possible to make the copyright management program automatically manage the data copyright in accordance with a data utilization condition held by the operating system without depending on an instruction of the user. According to the above constitution, a user can easily use a data copyright and the data copyright can more completely be managed.

Further, it is desirable that the copyright management program for managing the crypt key, data copyright information, the copyright label or the like is kept in a system area controlled by the operating system itself; i.e., the system area which the user program cannot access to.

Even in this case, however, if part of a data work is cut out and used, it is difficult to manage the data copyright. Therefore, when an operating system detects the such a situation, it is possible to manage the copyright of the cut-out part of the data by constituting a system so as to add copyright information and the copyright using attribute owned by original data to the cut-out part of the data by the copyright management program.

Further, to allow the cut-out data to inherit the copyright of the original data work, a "has-a" link, which is a parent and child relationship, is formed between the cut-

out data and the original data work with the copyright management program.

With such a constitution, it is possible to allow the new data to inherit the copyright of each original data work in the case where the user cuts out and incorporates his own desired portion from a plurality of copyright data to produce new data.

[Embodiment 16]

Because a copyright is a kind of property right, it is a matter of course that the charging for using the copyright occurs. Further, services such as offering of a secret-key and a copyright management program should be performed for pay.

The simplest method for paying these charges is a combination of issue of a bill and payment. However, this method is complex in its operation and moreover may cause a trouble such as nonpayment though the charge for using a copyright is directly paid.

There is a charge collection substituting method performed such as by a communication line enterprise, which is simple and has only a small risk of nonpayment because charges are collected by the communication line enterprise. However, it is necessary to pay a commission for charge collection substitution because charges are not directly collected.

To solve the above problem, there is a method for using digital cash. The digital cash is digital data used instead of cash in a computer connected to a c ommunication network, which is encrypted and used.

[Embodiment 17]

Further, the constitution of the data copyright management system described above can be applied not only to the data distribution but also to the distribution of the digital cash.

The digital cash system which has been proposed so far is based on a secret -key cryptosystem. The encrypted digital cash data is transferred from a bank account or a cash service of a credit company, and is stored in the IC card so that a terminal device for input/ output is used to make a payment. The digital cash system which uses this IC card as a cash-box can be used at any place such as shops or the like as long as the input/ output terminal is installed. However, the system cannot be used at places such as homes or the like where no input/output terminal is installed.

Since the digital cash is an encrypted data, any device can be used as the cash-box which stores digital cash data, in addition to the IC card, as long as the device can store encrypted data and transmit the data to the party to which the payment is made. As a terminal which can be specifically used as the cash-box, there are personal computers, intelligent television sets, portable telephone sets such as personal digital assistant (PDA), personal handyphone system (PHS), intelligent telephone sets, and PC cards or the like which has an input/ output function.

Trades in which such terminals are used as a cash-box for a digital cash can be actualized by replacing in the constitution of the data copyright control system, the database 1 with a customer's bank, a first user terminal 4 with a customer, the second user terminal 5 with a retailer, the copyright control center 18 with a retailer's bank and a third user terminal 6 with a wholesaler or a maker.

Further, it is desirable that the digital cash is processed as an object associated with data and functions instead of being as a simple data.

In handling a digital cash, there are a common digital cash form, an unentered digital cash form private for an owner, an entry column in the digital cash form private for the owner, a digital cash data showing an amount of money, an instruction of handling digital cash, and a digital cash form private for the owner in which an amount of money is entered. In an object-oriented programming, concepts such as an object, a class, a slot, a message and an instance are used.

In these correspondence relations, the common digital cash form becomes an object, the unentered digital cash form private for an owner becomes a class, the entry column of a digital cash form private for the owner becomes a slot, the instruction of handling digital cash becomes a message and the digital cash form private for the owner in which an amount of money is entered becomes an instance.

A digital cash data comprising the amount of money and the like is used as an argument. Then, the data is transferred and stored in a slot which is referred to as an instance variable by the message so that a new instance is made which is a digital cash in which the amount of money is renewed.

The digital cash which constitute an object will be specifically explained by using Figure 7.

In Figure 7, reference numerals 23, 25 and 27 represent a digital cash form private for the customer in which the amount of money stored in a customer terminal is entered, 29 represents a digital cash form private for the retail shop in which the amount of money stored in a retail shop terminal is entered, and 24, 26 and 28 represents accounts of each customer's bank.

A customer 23 draws out necessary amount of money from the account 24 to use the digital cash, and transfers the drawn out data 31 of the digital cash to the digital cash form 23 which is stored in the terminal.

In this case, residual amount data 30 of the digital cash is usually entered in the digital cash form 23. The digital cash form is not a class but an instance. The drawn out data 31 of the digital cash is transferred as an argument to the slot which is an entry column of the digital cash form 23 with the message instructing the addition to the residual amount data 30 of the digital cash. Then the drawn out data 31 of the digital cash is added to the residual amount data 30 of the digital cash in the digital cash form 23 so that a new instance is produced in which

the amount of money in the entry column of the digital cash form 23 is changed.

In the case where the customer makes a payment to the retail shop, the payment data 32 of the digital cash which corresponds to the paid amount is transferred as an argument to the slot which is an entry column of the digital cash form 23 with the message instructing the subtraction from the amount in the entry column of the digital cash form 23. Then payment data 32 of the digital cash is subtracted from the residual amount data 30 and the drawn out data 31 in the digital cash form 23 so that a new instance is produced in which the amount of money in the entry column of the digital cash form 23 is changed.

Further, the payment data 32 of the digital cash is transferred to the digital cash form 29 private for the retail shop.

A similar drawing out processing and payment processing are performed by digital cash forms 25 and 27 of other customers. The payment data 33 of the digital cash is transferred from the digital cash form 25, and the payment data 34 of the digital cash is transferred from the digital cash form 27 to the digital cash form 29 private for the retail shop.

In case of the digital cash 29 private for the retail shop, the residual amount data 35 of the digital cash is usually entered. The payment data 32 of the digital cash, the payment data 33 of the digital cash, and the payment data 34 of the digital cash are transferred as arguments to the slot which is an entry column of the digital cash form 29 with the message instructing the addition to the residual amount data 35 of the digital cash so that the payment data 32, 33 and 34 of the digital cash are added to the residual amount data 35 of the digital cash, and a new instance is produced in which the amount of money in the entry column of the digital cash form 29 is changed.

In a normal object-oriented programming, it is impossible that an argument is transferred to a slot with the message so that a new instance is produced and the newly produced instance as a whole is transferred. However, in case of the digital cash, since the cryptosystem is used for safety, an instance can be produced in which the payment data of the digital cash is entered at the payer. This instance can be encrypted and transferred to the payee.

An embodiment of the trading system will be explained in which the digital cash is transferred via a communication network by using Figure 8.

The embodiment is a modification of embodiment 9 by using a system constitution shown in Figure 4. In Figure 4, reference numeral 36 represents a customer, 37 a bank of the customer 36, 38 a retail shop, 39 a bank of the retail shop 38, 40 a maker, 41 a bank of the maker 40, 8 a public line provided by a communication enterprise or a communication network such as CATV line provided by a cable television enterprise. Customer 36, the customer's bank 37, the retail shop 38, the retail shop's bank 39, the maker 40, the maker's bank 41 can be mutually connected with the communication network 8. In this system, the customer 36 can use a credit company offering cashing service other than banks and he can also interpose appropriate number of wholesalers between the retail shop and the maker.

In addition, 42 and 43 are either IC cards or PC cards in which digital cash data is stored. The cards are used when the communication network is not u sed.

Incidentally, in Figure 8, what is represented by a broken line is a path of encrypted digital cash data, what is represented by the solid line is a path of requests from the customer, the retail shop or the maker, and what is represented by a one-dot chain line is a path of the secret-key from each bank.

Further, in this embodiment, the first secret-key prepared by the customer's bank 37, the second secret-key generated by the customer, the third s ecret-key generated by the retail shop, and the fourth secret-key prepared by the maker are used as crypt keys.

In this embodiment, the customer's bank 37, the retail shop's bank 39, and the maker's bank 41 are explained as separate entities. These can be considered as a financial system as a whole.

The digital cash management program P for encrypting and decrypting the digital cash data is preliminarily distributed to the customer 36 and is stored in the user terminal. Further, it is possible to transfer the digital cash management program P together with data every time trade with the bank is executed. Further, it is desirable to install the common digital cash programs P in all banks.

The customer 36 uses the user terminal to designate the amount of money via the communication network 8 to request drawing out from the account of the customer's bank 37 to the bank. At this time, the terminal presents customer information Ic.

The customer's bank 37 which receives the customer's request of drawing out from the account selects or generates the first secret-key Ks1 so that the digital cash data M0 of the amount is encrypted by the first secret-key Ks1:

$$Cm0ks1=E(Ks1, M0)$$

and the encrypted digital cash data Cm0ks1 and the first secret-key Ks1 for a decrypting key are transferred to the customer 36, and the customer information Ic and the first secret-key Ks1 are stored.

In this case, the first secret-key Ks1 can be selected from what is preliminarily prepared by the customer's bank 37, and also may be generated by p resentation of the customer information Ic at the time of drawing of the customer using the digital cash management program P on the basis of the customer information Ic:

$$Ks1=P(Ic).$$

Through this means, the first secret-key Ks1 can be private for the customer 36. At the same time, it is not necessary to transfer the first secret -key Ks1 to the cus-

tomer 36 so that the safety of the system can be heightened.

Further, the first secret-key Ks1 can be generated on the basis of the bank information Ibs of the customer's bank 37 or on the basis of the bank information Ibs and the date of key generation.

The customer 36 to which the encrypted digital cash data Cm0ks1 and the first secret-key Ks1 are transferred generates the second secret-key Ks2 according to any one or both of the customer information Ic and the first secret -key Ks1 using the digital cash management program P:

$$Ks2=P(Ic)$$

and the generated second secret-key Ks2 is stored in the user terminal.

Further, the customer 36 uses the secret-key Ks1 to decrypt the encrypted digital cash data Cm0ks1 with the digital cash management program P:

$$M0=D(Ks1, Cm0ks1)$$

and the content is confirmed. When the decrypted digital cash data M0 whose content is confirmed is stored in the user terminal which is a cash-box, the generated second secret-key Ks2 is used to encrypt the content by the digital cash management program P:

$$Cm0Ks2=E(Ks2, M0).$$

Incidentally, the first secret-key Ks1 is disused at this time.

The customer 36 who wishes to buy an article from the retail shop 38 decrypts the encrypted digital cash data Cm0ks2 which is stored in the user terminal as a cash-box by the digital cash management program P by using the second secret-key Ks2:

$$M0=D(Ks2, Cm0ks2)$$

and the digital cash data M1 which corresponds to the necessary amount of money is encrypted by the second secret-key ks2 using the digital cash management program P:

$$Cm1ks2=E(Ks2, M1)$$

and then, the payment is made by transmitting the encrypted digital cash data Cm1ks2 to the user terminal as a cash-box of retail shop 38 via the communication network 8.

At this time, the customer information Ic is also transmitted to the user terminal of the retail shop 38.

Further, the residual amount digital cash data M2 is encrypted by the second secret-key Ks2 using the digital cash management program P:

$$Cm2ks2=E(Ks2, M2)$$

and stored in the user terminal of the customer 36.

The retail shop 38 to which the encrypted digital cash data Cm1ks2 and the customer information Ic are transferred stores the transferred encrypted digital cash data Cm1ks2 and customer information Ic in the user terminal. At the same time, the customer information Ic is presented to the retail shop's bank 39 via the communication network 8 for confirming the content and the transmission for decription key is requested.

The retail shop's bank 39 which is requested by the retail shop 38 to transmit the second secret-key Ks2 transmits the request of the transmission of the second secret-key Ks2 and the customer information Ic to the customer's bank 37.

The customer's bank 37 which is requested to transmit the second secret-key Ks2 from the retail shop's bank 39 generates the second secret-key Ks2 according to the customer information Ic by the digital cash management program P in the case where the second secret-key Ks2 is based only on the customer information Ic, or generates the second secret-key Ks2 according to the customer information Ic and the first secret-key Ks1 by the digital cash management program P in the case where the second secret-key Ks2 is based on the customer information Ic and the first secret-key Ks1, and transmits the generated second secret-key Ks2 to the retail shop's bank 39.

The retail shop's bank 39 to which the second secret-key Ks2 is transmitted from the customer's bank 37 transmits the second secret-key Ks2 to the retail shop 38 via the communication network 8.

The retail shop 38 to which the second secret-key Ks2 is transferred decrypts the encrypted digital cash data Cm1ks2 by the second secret-key Ks2 using the digital cash management program P:

$$M1=D(Ks2, Cm1ks2)$$

and after confirming the amount of money, transfers the article to the customer 36.

Incidentally, in this case, the retail shop 36 can directly requests the transfer of the second secret-key Ks2 to the customer's bank 37 instead of the retail shop's bank 39.

In case where the digital cash received by the retail shop 38 is deposited in the account of the retail shop's bank 39, the customer information Ic is transferred to the retail shop's bank 39 together with the encrypted digital cash data Cm1ks2 via the communication network 8.

The retail shop's bank 39 to which the encrypted digital cash data Cm1ks2 and the customer information Ic are transferred requests the transfer of the second secret-key Ks2 to the customer's bank 37 by transmitting the customer information Ic.

The customer's bank 37, which is requested to transfer the second secret-key Ks2 from the retail shop's bank 39, generates the second secret-key Ks2 according to the customer's information Ic by the digital cash management program P when the second secret-key Ks2 is

only based on the customer's information Ic, or generates the second secret-key Ks2 according to the customer's information Ic and the first secret-key Ks1 by the digital cash management program P when the second secret-key Ks2 is based on the customer's information Ic and the first secret-key Ks1, then the generated second secret-key Ks2 is transferred to the retail shop's bank 39.

The retail shop's bank 39, to which the second secret-key Ks2 is transferred from the customer's bank 37, decrypts the encrypted digital cash data Cm1ks2 by the second secret-key Ks2 using the digital cash management program P:

$$M1=D(Ks2, Cm1ks2)$$

and the decrypted digital cash data M1 is deposited in the bank account of the retail shop 39.

In the general trade system, the retail shop 38 stocks products from the maker 40 or from the whole sale shops which intervene between the retail shop 38 and the maker 40. Then the retail shop 38 sells the products to the customer 36. Consequently, a trading form is present between the customer 36 and the retail shop 38 just as between the retail shop 38 and the maker 40.

The handling of the digital cash between the retail shop 38 and the maker 40 is not basically different from the handling of the digital cash which is carried out between the customer 36 and the retail shop 38. Therefore, the explanation there will be omitted for the sake of clarity.

In this digital cash system, the digital cash is handled through bank. As information such as the processed amount of the digital cash, date, and the secret-key demanding party information with respect to the handling of the digital cash is stored in the customer's hank, the residual amount and usage history can be grasped.

Even in the case where the user terminal which is a cash-box storing the digital cash data cannot be used owing to the loss or the breakage, it is possible to reissue the digital cash on the basis of the residual amount, and usage history kept in the customer's bank.

It is desirable to add a digital signature to the digital cash data for heighten the safety of the digital cash.

In this embodiment, digital cash is added by the customer's information which may be accompanied by digital signature. Therefore, the digital cash in the embodiment can also have a function of settlement system for checques drawn by customers.

Also this system can be applicable to various systems such as a negotiation of a draft by a letter of credit and a bill of lading in the international trading, which have been executed by documents.

[Embodiment 18]

The digital cash in the digital cash system which is explained in embodiment 17 is always handled through bank. However, since it is possible to handle the digital cash without bank intervention, the digital cash system in which the bank does not intervene will be explained.

In the digital cash system, a public-key and a private-key are used as crypt keys for encrypting the digital cash data. The secret-key ks and customer information 1c used in embodiment 17 is not used.

Consequently, in this digital cash system, the digital cash is used in the same form as money.

Since other points are not different from the system constitution shown in embodiment 17, concrete explanation is omitted.

The party which receives the digital cash at each bank, customer, retail shop and maker with respect to this digital cash system prepares the public-key and the private-key. The public-key can be preliminarily sent to the party which is scheduled to make a payment, or can be sent to the party before the trade is executed. Here an explanation is made on the supposition that the key is preliminarily distributed.

The customer 36 requests to the customer's bank 37 for drawing out the money from the bank account via the communication network 8 from a user terminal, by indicating an amount of the money.

The customer's bank 37 which receives the request for drawing out money from the customer 36 encrypts the digital cash data Mo of the amount of money drawn by a customer public-key Kbc which is preliminarily sent, using the digital cash management program P

$$Cm0kbc=E(Kbc, M0)$$

and transfers the encrypted digital cash data Cm0kbc to the customer 36.

The customer 36 to which the encrypted digital cash data Cm0kbc is transferred decrypts the digital cash data by the customer private-key Kvc which corresponds to the customer public-key Kbc using the digital cash management program P:

$$M0=D(Kvc, Cm0kbc),$$

confirms the content, and changes the residual amount to M2(=M0+M1) in the case where there is a residual amount data M1 in the terminal. Then, the digital cash data M2 in which the amount of money is changed is encrypted with the customer public-key Kbc with the digital cash management program P:

$$Cm2kbc=E(Kbc, M2)$$

and stored in the terminal.

The customer 36 who wishes to buy products from the retail shop 38 decrypts the encrypted digital cash data Cm2Kbc stored in the terminal by the customer private-key Kvc using the digital cash management program P:

$$M2=D(Kvc, Cm2kbc),$$

encrypts the digital cash data M3 corresponding to the required amount of money with the digital cash management program P by the retail shop public-key Kbs which is preliminarily sent:

$$Cm3kbs=E(Kbs, M3)$$

and the payment is made by transferring the digital cash data to the terminal of the retail shop 38 via the communication network 8.

Further, the residual amount digital cash data M4(=M2-M3) is encrypted by the customer public-key Kbc using the digital cash management program P

$$Cm4kbc=E(Kbc, M4)$$

and stored in the terminal.

The retail shop 38 to which the encrypted digital cash data Cm3Kbs is transferred decrypts the digital cash data with the digital cash management program P by the retail shop private-key Kvs corresponding to the retail shop public-key Kbs:

$$M3=D(Kvs, Cm3kbs),$$

confirms the content and changes the residual amount data to M6(M5+M3) in the case where the residual amount data M5 is present in the terminal. Then, the digital cash data M6 in which the amount of money is changed is encrypted with the retail shop public-key Kbs with the digital cash management program P:

$$Cm6kbs=E(Kbs, M6)$$

and stored in the terminal.

The retail shop 38 which is willing to settle the stock account of products to the maker 40 makes the settlement using the same manner.

In the general trade system, the retail shop 38 stocks products either from the maker 40 or the wholesaler placed between the retail shop 38 and the maker 40 and sells the products to the customer 36.

Consequently, a trade form similar to the trade form between the customer 36 and the retail shop 38 is present between the retail shop 38 and the maker 40.

Since the handling of the digital cash between the retail shop 38 and the maker 40 is not basically different from the handling of digital cash between the customer 36 and the retail shop 38, an explanation is omitted for the sake of clarity.

In the aforementioned embodiment 17 and embodiment 18, a constitution of a data copyright management system explained by using Figure 4 is applied to actualize the digital cash system. Further, customer information is used and the secret-key to be used is altered in embodiment 17, and the public-key and the private-key are used in embodiment 18.

However, as a system constitution for actualizing the digital cash system, the constitution of the other copyright management systems, any constitution of the data copyright management system shown in Figure 1, 2, 3 and 5 can be applied. Further, as a cryptosystem used in the case, any of the cryptosystems explained in embodiments 1 through 13 using the non-altered secret -key, the public-key and the private-key, a combination of the secret-key, publi c-key and the private-key, and complex keying can be applied.

[Embodiment 19]

In the video conference system, a television picture has been added to the conventional voice telephone set. Recently the video conference system is advanced in which a computer system is incorporated in the video conference system so that the quality of the voice and the picture are improved, and data can be handled at the same time as well as the voice and the picture.

Under these circumstances, security against the violation of the user's privacy and the data leakage due to eavesdropping by persons other than the participants of the conference are protected by the cryptosystem using a secret-key.

However, since the conference content obtained by the participants themselves are decrypted, in the case where participants themselves store the content of the conference and sometimes edit the content, and further, use for secondary usage such as distribution to the persons other than the participants of the conference; the privacy of other participants of the video conference and data security remains unprotected.

In particular, the compression technology of the transmission data is advanced while the volume of the data storage medium is advanced with the result that the possibility is getting more and more realistic that all the content of the video conference is copied to the data storage medium or is transmitted via a network.

In view of the circumstances, embodiment 19 is intended, when video conference participants perform secondary use, to secure the privacy of other participants and data security by using the aforementioned constitution of the data copyright management system.

This video conference data management system can be actualized, for example, by replacing the database 1 in the data copyright management system constitution shown in Figure 4 with a participant of the video conference, the first user terminal 4 with another participant of the video conference, and the second user terminal 5 with non-participant of the video conference.

Embodiment 19 will be explained by using Figure 9.

Referring to Figure 9, reference numeral 44 represents a participant as a host of the video conference, 45 a participant of the video conference as a guest, 46 a non-participant of the video conference as a user, 47 a non-participant of the video conference as another user, 8 a communication network such as a public telephone line provided by the communication enterprise and a CA television line provided by the cable television enterprise or the like. The participant 44 of the video conference is

connected to the participant 45 of the video conference via the communication network 8. Further, the participant 45 of the video conference can be connected to the non-participant 46 of the video conference, and the non-participant 46 of the video conference to the non-participant 47 of the video conference, via the communication network 8. Reference numeral 48 represents a data recording medium.

Referring to Figure 9, what is represented by the broken line is a path of the encrypted video conference content, represented by the solid line is a path requesting the crypt key from the non-participants 46 and 47 of the television conference to the participant of the television conference 44, and represented by the one-dot chain line is a path of crypt keys from the participant of the video conference 44 to the participant of the video conference 45 and the non-participants of the video conference 46 and 47.

In this embodiment, a video conference data management system is described here only the protection for data security and privacy in case of the video conference participant 44 to simplify the explanation, however, it is of course, possible to protect for data security and privacy of the video conference participant 45.

A video conference data management program P for encryption/decryption of the video conference data is previously distributed to the video conference participant 45 and the video conference non-participants 46 and 47, and is stored in each terminal. The video conference data management program P may be transferred whenever a crypt key is transferred.

In this embodiment, further, a first secret-key prepared by the video conference participant 44, a second secret-key prepared by the video conference participant 45 and a third secret-key prepared by the video conference non-participant 46 are also used.

The video conference participant 44 and the video conference participant 45 perform the video conference by transmitting audio, picture and data (referred to as video conference data on the whole) each other, using each terminal via communicatin network 8. Before the video conference, the video conference participant 44 generates or selects the first secret-key Ks1 to transfer to the video conference participant 45 prior to the start of the video conference.

The video conference participant 45 receiving the first secret-key Ks1 generates the second secret-key Ks2 by the first secret-key Ks1 using the video conference data management program P:

$$Ks2=P(Ks1).$$

The generated second secret-key Ks2 is stored in the terminal.

The participant 44 of the video conference encrypts the video conference data M0 with the first secret-key Ks1 in the video conference via the communication network 8:

$$Cm0ks1=E(Ks1, M0)$$

and transfers the encrypted video conference data Cm0ks1 to the video conference participant 45.

The participant 45 of the video conference who receives the video conference data Cm0ks1 encrypted by the first secret-key Ks1 decrypts the video conference data Cm0ks1 by the first secret-key Ks1:

$$M0=D(ks1, Cm0ks1)$$

and uses decrypted video conference data M0.

Further, the second secret-key Ks2 is generated based on the first secret-key Ks1 with the video conference data management program P:

$$Ks2=P(Ks1).$$

In the case where the decrypted video conference data M0 is stored in the terminal of the participant 45 of the video conference, copied to the data record medium 48, or transferred to the non-participant of the video conference via the communication network 8, the data M is encrypted by the second secret-key Ks2 using the video conference data management program P:

$$Cmks2=E(Ks2, M).$$

The encrypted data Cmks2 is copied to the record medium 48 or supplied to the non-participant of the video conference via the communication network 8, together with the video conference data name or the video conference data number.

The non-participant 46 of the television conference who obtains the encrypted data CmKs2 requests to the participant 44 for the secondary use of the video conference data M from the terminal by specifying the name or number of the video conference data.

The participant 44 of the video conference who receives the request for the second use of the data M finds out the first secret-key Ks1 according to the name or the number of the video conference data name or number to generate the second secret-key Ks2 based on the first secret-key Ks1:

$$Ks2=P(Ks1)$$

and supplies the generated second secret-key Ks2 to the non-participant 46 of the video conference.

The non-participant 46 of video conference who receives the second secret-key Ks2 decrypts the encrypted data Cmks2 by the second secret-key Ks2 by using the television conference data management program P:

$$M=D(Ks2, Cmks2)$$

and then, uses decrypted video conference data M.

In the case where the video conference data M is stored in the terminal of the non-participant 46 of the video conference, copied to the record medium 49, or transmitted to the non-participant 47 of the video conference, the video conference data M is encrypted by the second secret-key Ks2 using the video conference data management program P:

$$Cmks2=E(Ks2, M).$$

Incidentally, the third secret-key Ks3 may be generated on the basis of the second secret-key Ks2 with the television conference data management program P:

$$Ks3=P(Ks2),$$

and the data M can be encrypted with the video conference data management program P by this generated third secret-key Ks3:

$$Cmks3=E(Ks3, M).$$

In embodiment 19 described above, the constitution of the data copyright management system which is explained by using Figure 4 for realizing the video conference data management system is applied and alter the secret-key which has been used.

However, as a constitution of a system for realizing the video conference data system, as the other system constitution; i.e., any of system constitutions shown in Figure 1, 2, 3, 4 and 5 can be applied. Further, as cryptosystem used in such a case, the non-altered secret-key, the public-key and the private-key, a combination of the secret-key, the public-key and the private-key, and the complex keying which is explained from embodiment 1 to 13 can be applied.

Further, in this explanation, it is supposed that the participant of the video conference as a guest stores and uses the video conference data, copies the data on the record medium and transfers the data via the communication network. It is also possible to limit these actions by making the crypt key used in the encryption process be disused.

[Embodiment 20]

As described above, each user who uses the system of the present invention must previously be entered in a database system, and when entered in the system, software for database is supplied to the user.

Because the software includes not only normal communication software such as a data communication protocol but also a program for decrypting a copyright management program by a first crypt key, it is necessary to be protected.

In case of the present invention, a first crypt key K1, a second crypt key K2, and a copyright management program P are transferred to each user in order to use data M. Therefore, each user must keep these keys and the program.

Further, the copyright information label, user information, the public-key and private-key in the public-key cryptosystem and the program containing algorithm for generating the secret-key are kept when needed.

For keeping them, it is the simplest means to use a flexible disk. However, the flexible disk is easy in disappearance or alteration of data.

Moreover, a hard disk drive is also unstable for disappearance or alteration of data though it is more stable than the flexible disk.

Recently, an IC card is spread in which an IC element is sealed in a card-like package. Particularly, standardization of a PC card with a microprocessor sealed in it is progressed as a PCMCIA card or JEIDA card.

Figure 10 shows an embodiment of the database copyright management system of the present invention constituted by using the PC card.

In Figure 10, reference numeral 50 represents a microprocessor of a user terminal, 51 represents a system bus, and 52 represents a PC card in which a PC card microprocessor 53, a read-only memory 55, and a random-access memory 56 are sealed and these are connected each other by a PC card microprocessor bus 54.

The read-only memory 55 stores fixed information such as database software and user data as a database.

The read-only memory 55 also stores a first crypt key, a second crypt key, and a copyright management program supplied from a key control center 9 or a copyright management center. Because data is also written in the read-only memory 55, it is the simplest to use an EEPROM for the memory 55.

As previously described, because data, the crypt key the copyright management program can be encrypted and supplied to users, for using data, it is necessary to decrypt these crypt key, copyright management program and the data.

To perform the above operations, the microprocessor 50 of the user terminal uses the software, crypt key and copyright management program stored in the read-only memory 55 of the PC card 52.

In this case, however, there is a risk that these data informations may illegally be used because they are transferred to the user terminal. To avoid the risk, it is necessary to make the microprocessor 55 in the PC card 52 perform every operation by using the random-access memory 56 through the CPU bus 54 and transfer results only to the user terminal for various types of utilization.

When the PC card is used, a different unit can be used as the user terminal.

It is also possible to use a board or external unit having the above functions in addition to the PC card.

Claims

1. Data copyright management system for managing the copyright of encrypted data supplied from a database to a user, said data copyright management

system having the database 1 and a key control center 9;

wherein a key for decrypting said encrypted data is supplied from said key control center 9 to said user;

said user uses said key for decrypting when said user displays or editssaid data to decrypt said encrypted data; and

said data is re-encrypted when said user stores, copies or transfers said data or data which has been edited.

2. Data copyright management system according to claim 1 wherein said key used in said reencryption is different from said key for decryption.

3. Data copyright management system according to claim 1 or 2 wherein a copyright management program is further used for managing the copyright of said data.

4. Data copyright management system according to one of the preceding claims, wherein a data copyright management program is stored in a memory, selected from a ROM of a device which said user uses and a system area controlled by an operating system of the device which said user uses.

5. Data copyright management system according to one of the preceding claims, wherein further a copyright information which is not encrypted with respect to said data copyright is used.

6. Data copyright management system according to any of the preceding claims, wherein said non-encrypted copyright information is added to said encrypted data as a copyright information label, said copyright information label being stored, copied or transmitted together with said data if said data is stored, copied or transmitted.

7. Data copyright management system according to claim 6 wherein a digital signature is added to said copyright information label.

8. Data copyright management system for using data encrypted and supplied from a database to a user, comprising the database 1, a key control center 9 and a copyright management center 10;

wherein said data copyright management system uses secret-key, user information and copyright management program;

said database 1 encrypts the data with a first secret-key to distribute the data to a first user 4 via communication network 8, communication and broadcasting satellite 2 and record medium 3;

said first user 4 provides the first user information to said key control center 9 to request the use;

said key control center 9 transfers said first user information to said copyright management center 10;

said key control center 9 transfers the copyright management program together with said first secret-key and second secret-key to said first user 4 via said communication network 8;

said first user 4 uses said first secret-key with said copyright management program to decrypt said encrypted data for use; and

said data decrypted is re-encrypted if said decrypted data is stored, copied or transmitted with said copyright management program by using said second secret-key, and uncrypted first user information is added.

9. Data copyright management system according to claim 8 wherein said first secret-key and said second secret-key are disused with said copyright management program, when said decrypted data is copied or transmitted; and

said first user 4 requests for the retransfer of said second secret-key for the reuse of said reencrypted data to said copyright management center 10 so that said second secret-key is retransmitted.

10. Data copyright management system according to claim 9 wherein the copy or transmit of said encrypted data is registered in said copyright management center 10 according to the retransfer of said second secret-key.

11. Data copyright management system according to claim 9 or 10 wherein second user 5 presents said first user information to request the use to said copyright management center 10;

said copyright management center 10 transfers said second secret-key and third secret-key, and said copyright management program to said second user 5 after confirming the retransfer of said second secret-key to said first user 4;

said second user 5 decrypts said encrypted data with said copyright management program by using said second secret-key; and

said data is reencrypted and redecrypted with said copyright managementprogram by using said third secret-key when said decrypted data is stored, copied or transmitted.

12. Data copyright management system according to claim 8, 9, 10 or 11 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright management program with said copyright management program.

13. Data copyright management system for using data encrypted and supplied from a database to a user, said data copyright management system comprising

a database 1, a key control center 9 and a copyright management center 10;

wherein said data copyright management system uses secret-key, user information and copyright management program;

first user 4 presents the first user information to the database 1 to request the use of the data;

said database 1 encrypts said requested data by using first secret-key and transfers it to said first user 4 via said communication network 8 together with said first secret-key, second secret-key and said copyright management program;

said key control center 9 transfers said first user information to said copyright management center 10;

said key control center 9 transfers the copyright management program together with said first and second secret-keys to said first user 4 via said communication network 8;

said first user 4 decrypts and uses said encrypted data with said copyright management program by using said first secret-key; and

said decrypted data is re-encrypted when said decrypted data is stored, copied or transmitted with said copyright management program by using said second secret-key, and uncrypted first user information is added.

14. Data copyright management system according to claim 13 wherein said first and second secret-keys are disused with said copyright management program when said decrypted data is copied or transmitted;

said first user 4 requests retransfer of said second secret-key for thereuse of the reencrypted data to said copyright management center 10; and

said second secret-key is retransferred.

15. Data copyright management system according to claim 14 wherein the copy or transmit of said encrypted data is registered in said copyright management center 10 according to the retransfer of said second secret-key.

16. Data copyright management system according to claim 14 or 15 wherein second user 5 presents said first user information to request the use to said copyright management center 10;

said copyright management center 10 transfers said second secret-key, third secret-key and said copyright management program to said second user 5 after confirming the retransfer of said second secret-key to the first user 4;

said second user 5 decrypts said encrypted data with said copyright management program by using said second secret-key; and

said data is reencrypted and redecrypted with said copyright management program by using said third secret-key in the case where said decrypted data is stored, copied or transmitted.

17. Data copyright management system according to claim 13, 14, 15 or 16 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright management program with said copyright management program.

18. Data copyright management system for using data encrypted and supplied from a database to a user, comprising a database 1, a key control center 9 and a copyright management center 10;

said data copyright management system uses secret-key, public-key and private-key;

first user 4 presents first public-key, second public-key and first user information to request the use of the desired data to said key contrl center 9;

said database which receives the request for use encrypts said data by using first secret-key, encrypts said first secret-key by using said first public-key, and encrypts second secret-key by using said second public-key;

said encrypted data, said encrypted first secret-key, said encrypted second secret-key and said copyright management program are transmitted to said first user;

said first user decrypts said encrypted first secret-key by using first private-key, decrypts said encrypted data by using said decrypted first secret-key, and decrypts said encrypted second secret-key by using second private-key, with said copyright management program;

said data is encrypted and decrypted with said copyright management program by using the second secret-key in the case where said decrypted data is stored, copied or transmitted.

19. Data copyright management system according to claim 18 wherein said first and second secret-keys are disused with said copyright management program when said decrypted data is copied or transmitted;

said first user 4 who reuses said encrypted data requests for the retransfer of said second secret-key for the reuse of said reencrypted data to said copyright management center 10; and

said second secret-key is retransferred.

20. Data copyright management system according to claim 19 wherein the copy or transmit of said encrypted data is registered in said copyright management center 10.

21. Data copyright management system according to claim 19 or 20 wherein second user 5 presents said first user information to request the use to said copyright management center 10;

said copyright management center 10 transfers said second secret-key, third secret-key, and said copyright management program to said second user 5 after confirming the retransfer of said second secret-key to said first user 4;

said second user decrypts said encrypted data with said copyright management program by using said second secret-key; and

said data decrypted is reencrypted and redecrypted with said copyright management program by using said third secret-key in the case where said decrypted data is stored, copied or transmitted.

22. Data copyright management system according to claim 18 - 22 wherein said second secret-key is generated on the basis of any one or more of said first secret-key, said user information, and the usage frequency of said copyright management program.

23. Data copyright management system for using a plurality of data encrypted each by different secret-keys and supplied from database to a user, said system using a sycret-key, user information and a copyright management program, comprising:

first user 4 obtaining from a copyright management center 10 a plurality of copyright management programs unique to original said plurality of data anda plurality of first secret-keys to decrypt said plurality of original data with a plurality of said first secret-keys;

one or a plurality of second secret-keys being generated with a plurality of copyright management programs unique to said plurality of original data;

wherein said plurality of original data which are used or edited are encrypted with said one or a plurality of second secret-keys with said plurality of copyright management programs unique to said plurality of original data to be stored, copied or transmitted together with the edition process data; and

said plurality of original data or said plurality of edited data encrypted with said one or plurality of second secret-keys are decrypted with said one or plurality of second secret-keys and said plurality of copyright management programs obtained from said copyright management center 10 for second user 5 to use and edit by using said edition process.

24. Data copyright management system according to claim 23 wherein said second secret-key is generated with said copyright management program on the basis of any one or more of said first secret-keys and said user information.

25. Data copyright management system for using data encrypted and supplied from a database 1 to a user, using a crypt key, user information and a copyright management program, comprising:

said user presenting user information to said database 1;

said database 1 supplying said data encrypted with first crypt key to first user;

said first user generating a second crypt key based on said first crypt key with said copyright management program;

said encrypted data being decrypted by using said first crypt key in the case where said first user uses said encrypted data; and

said decrypted data being reencrypted by using said second crypt key in the case where said first user stores, copies or transmits said decrypted data.

26. Data copyright management system according to claim 25 wherein said crypt key is selected from the group comprising a secret-key and a public-key and a private-key.

27. A digital cash management system for using digital cash encrypted and supplied from a financial organization to first user, comprising:

said financial orginization supplying a key for decrypting said encrypted digital cash data to said first user;

Decrypting of said digital cash data by using said decrypting key in the case where said first user confirms said digital cash data; and

Reencrypting said data if said first user stores said decrypted digital cash data, if changed digital cash data is stored, or if digital cash data is transmitted to said second user.

28. A digital cash management system according to claim 27 wherein the key used in said reencryption is a crypt key which is different from said decrypting key.

29. A digital cash management system according to claim 27 or 28 wherein further a digital cash management program is used for managing said digital cash.

30. A digital cash management system according to claim 27, 28 or 29 wherein further a not encrypted first user information is used.

31. A digital cash management system according to claim 27, 28, 29 or 30 wherein said not-encrypted first user information is added to said encrypted digital cash data as the first user information label to be stored or transmitted together with said digital cash data if said digital cash data is stored, if changed digital cash data is stored, or if said digital cash data is transmitted to the second user.

32. A digital cash management system according to claim 31 wherein a digital signature is added to said first user information label.

33. A digital cash management system for using digital cash encrypted and supplied from a financial organization to a first user, said system using a crypt key, user information and digital cash management program, comprising:

said first user presenting the first user information to said financial organization;

said financial organization providing said first user with said digitalcash data encrypted by the first crypt key;

wherein said first user generates a second crypt key on the basis of said first crypt key with said digital cash management program;

said encrypted digital cash data is decrypted by using said first crypt key in the case where said first user confirms said encrypted digital cash data;

said digital cash data decrypted is reencrypted by using said second crypt key to be stored said first user;

said decrypted digital cash data is reencrypted by using said second crypt key and said digital cash data reencrypted is transmitted to second user together with said first user information in the case where said decrypted digital cash data is transmitted to said second user;

said first user information is presented to said financial organization from said second user;

said financial organization generates said second crypt key based on said first user information and transfers said second crypt key to said second user; and

said second user decrypts said reencrypted digital cash data with said digital cash management program by using said second crypt key which is transferred.

34. A digital cash management system according to claim 33 wherein said crypt key is selected from the group comprising a secret-key and a public-key and a private-key.

35. A digital cash management system for using a digital cash encrypted and supplied from a financial organization to first user, said system using a public-key and a private-key, comprising:

said first user presenting first public-key to said financial organization;

said financial organization encrypting digital cash data with said first public-key to supply to said first user;

said first user decrypting said digital cash data by using first private-key;

second user presenting second public-key to said first user;

said first user encrypting said digital cash data which is decrypted with said second public-key to transfer to said second user; and

said second user decrypting said digital cash data by using second private-key.

36. A video conference data management system for using video conference data encrypted and supplied from first user to second user, comprising:

a key for decrypting said encrypted video conference data being supplied from said first user to said second user;

said encrypted video conference data being decrypted by using said decrypting key in the case where said second user uses said video conference data; and

said data being reencrypted in the case where said second user stores decrypted said video conference data, in the case where edited video conference data is stored, or in the case where said video conference data is transmitted to third user.

37. A video conference data management system according to claim 36 wherein a crypt key used for said re-encryption is different from said decrypting key.

38. A video conference data management system according to claim 36 or claim 37 wherein a video conference data management program for managing said video conference data is further used.

39. A video conference data management system according to claim 35, 36 or 37 wherein further non-encrypted first user information is used.

40. A video conference copyright management system according to claim 36, 37, 38 or 39 wherein said uncrypted first user information is added to said encrypted video conference data as the first user information label which is copied or transmitted together with said video conference data in the case where said video conference data is stored, in the case where the edited video conference data is stored, or in the case where the video conference data is transmitted to third user.

41. A video conference data management system according to claim 40 wherein a digital signature is added to said first user information label.

42. A video conference data management system for using video conference data encrypted and supplied from first user to second user, said system using a crypt key, user information, and video conference data management program:

wherein said second user presents second user information to said first user;

said first user supplies to said second user said video conference data encrypted with the first crypt key;

said second user uses said video conference data management program to generate the second crypt key based on said first crypt key;

said encrypted video conference data is

decrypted by using said first crypt key in the case where said second user uses said encrypted video conference data; and

said decrypted video conference data is reencrypted by using said second crypt key in the case where said second user stores, copies or transmits said decrypted video conference data.

43. A video conference data management system according to claim 42 wherein said crypt key is selected from the group concerning a secret-key and a public-key and a private-key.

44. Data copyright management apparatus connected for use to a system bus in main body of user terminal, comprising a microprocessor, a read only memory, reading and writing memory and EEPROM connected to a microprocessor bus:

said read only memory storing fixed information such as database utilization software and user data or the like; and

said EEPROM storing first crypt key, second crypt key and a copyright management program supplied from a key control center or a copyright management center.

FIG. 1

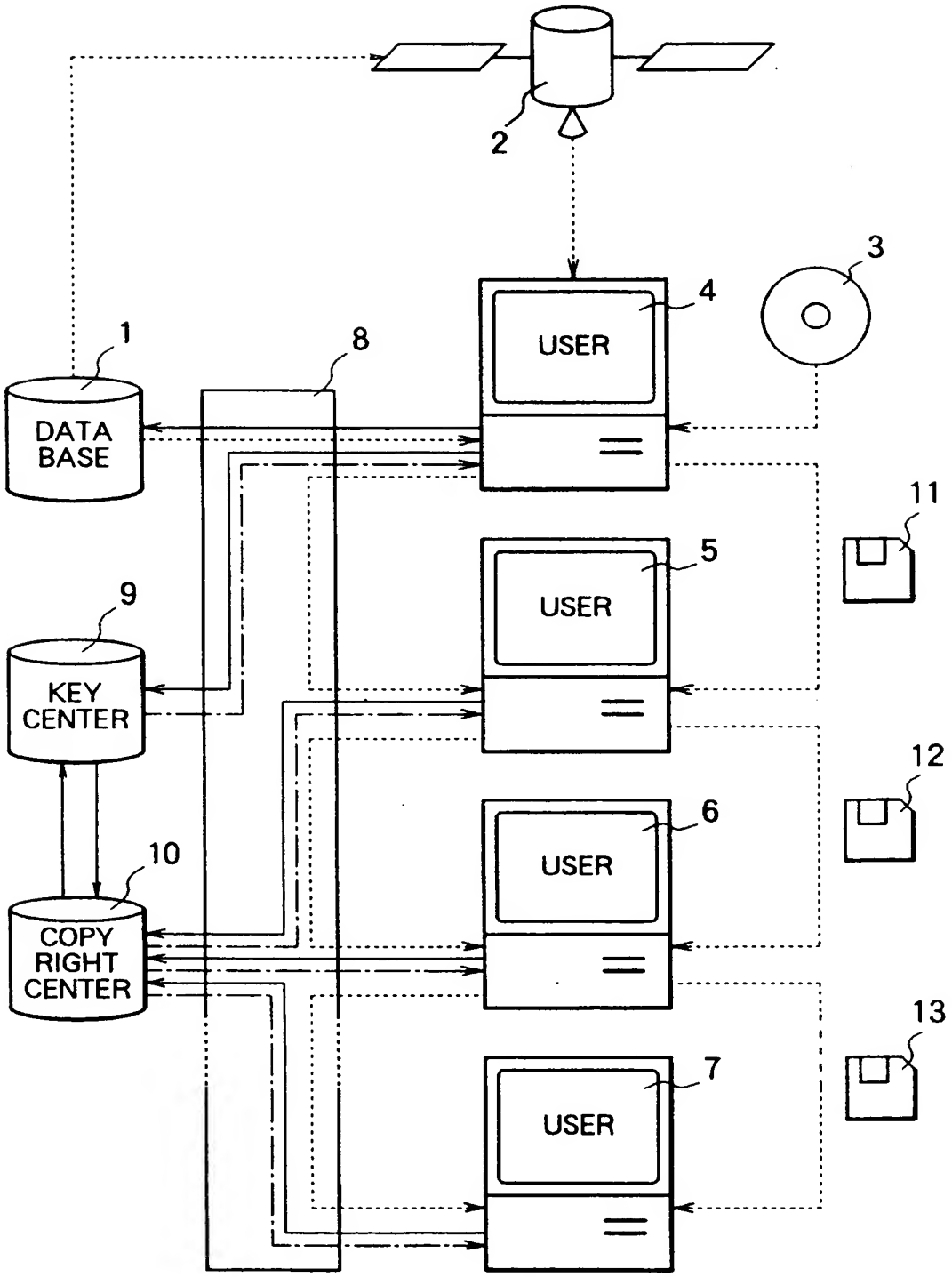


FIG. 2

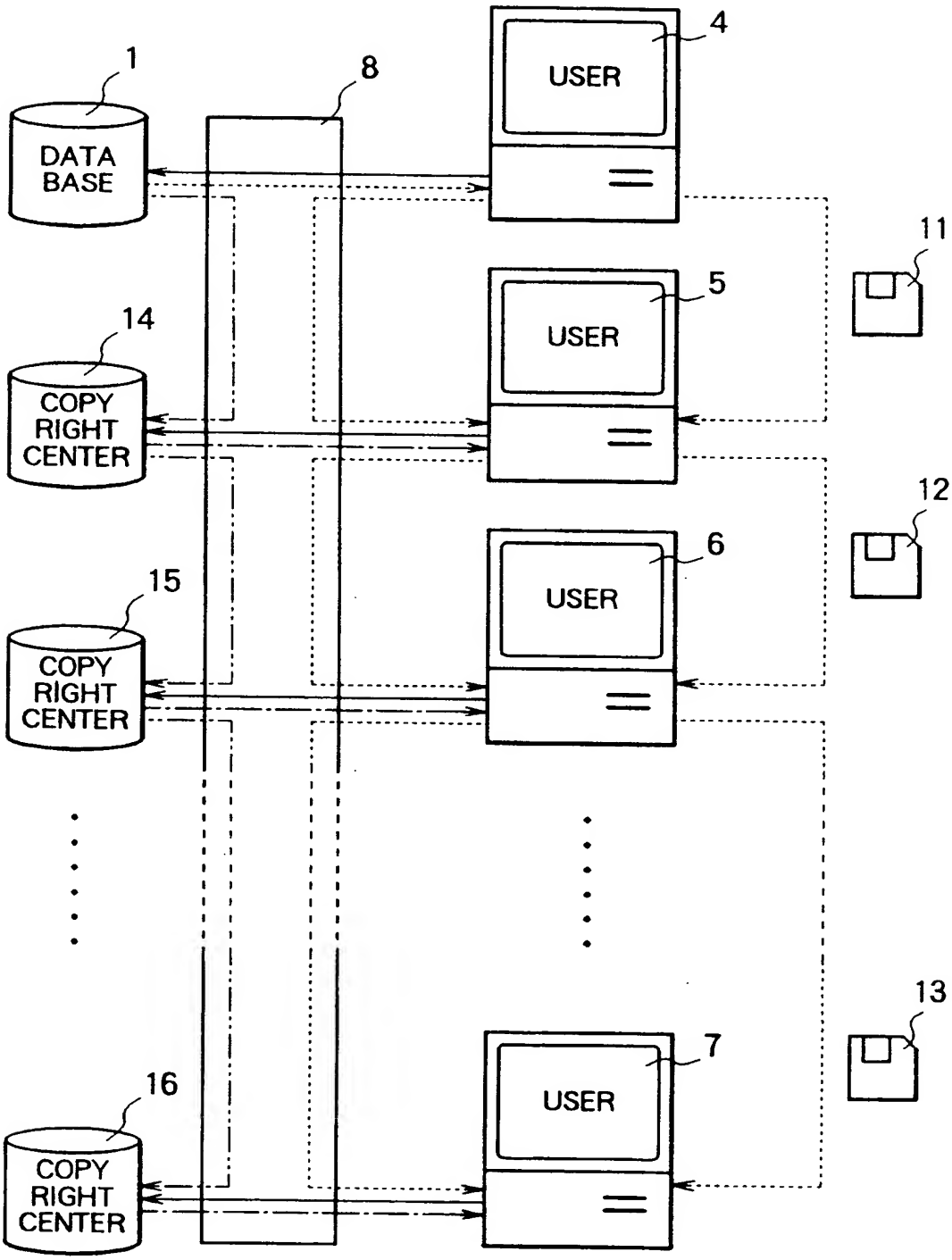


FIG. 3

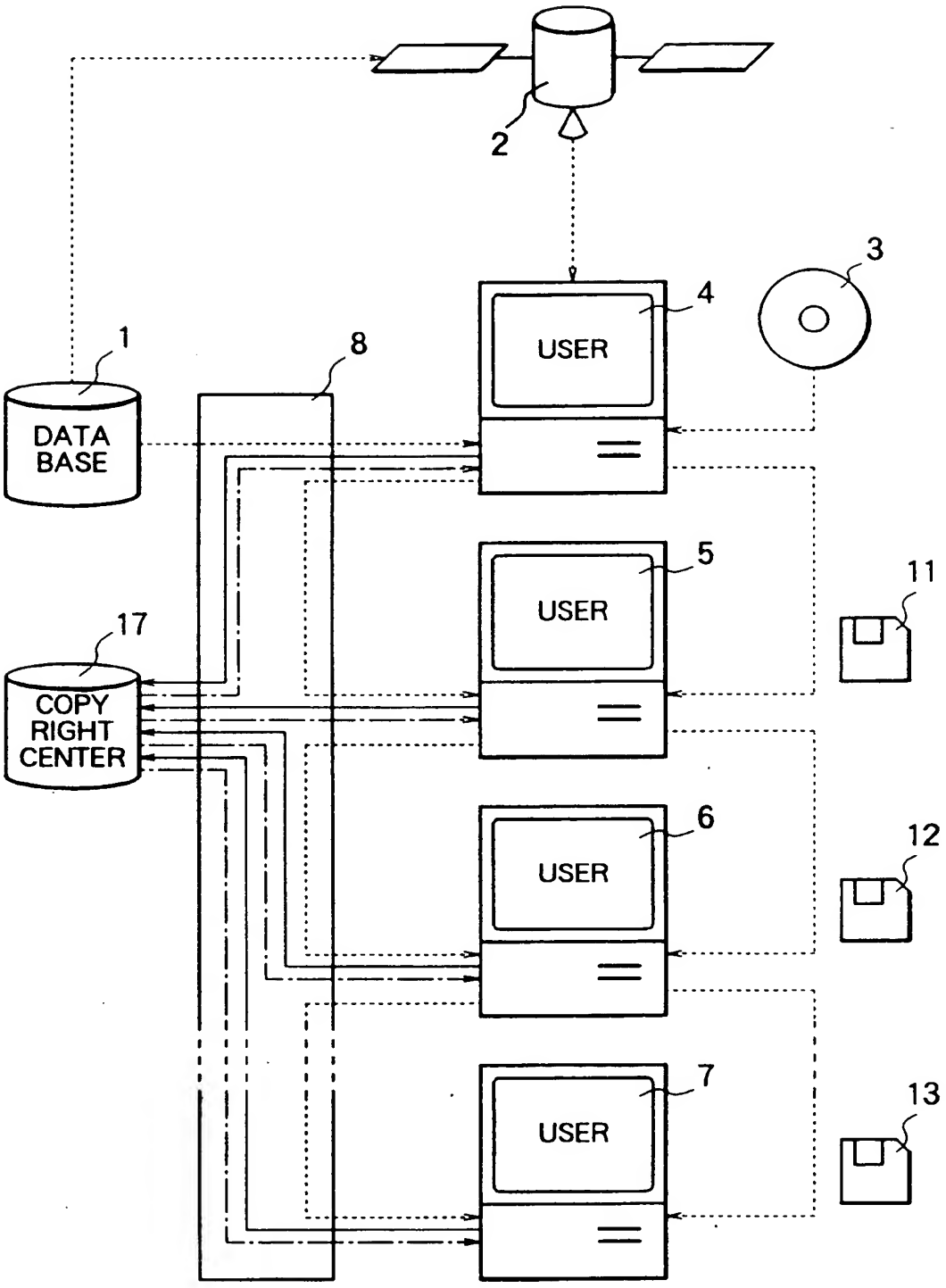


FIG. 4

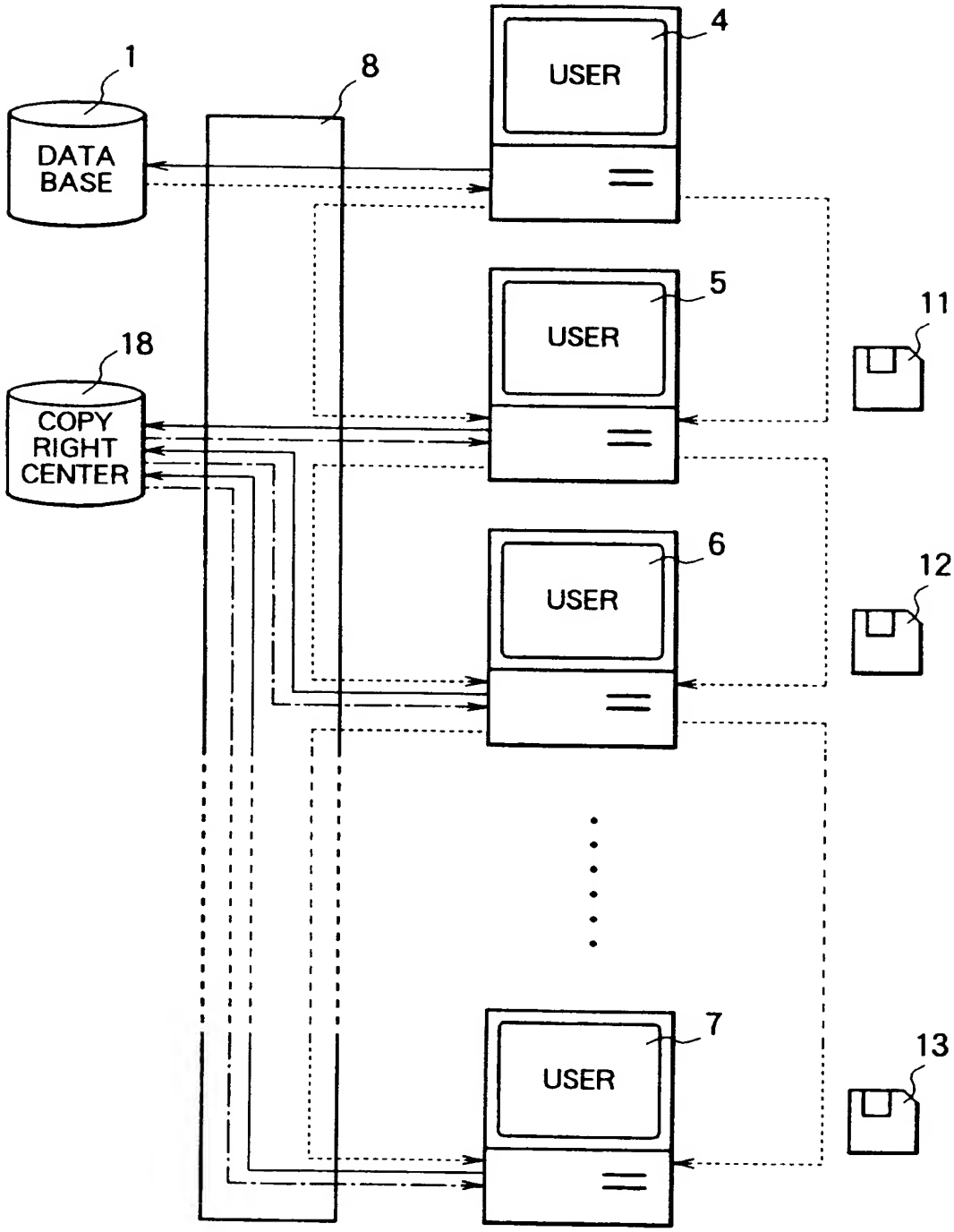


FIG. 5

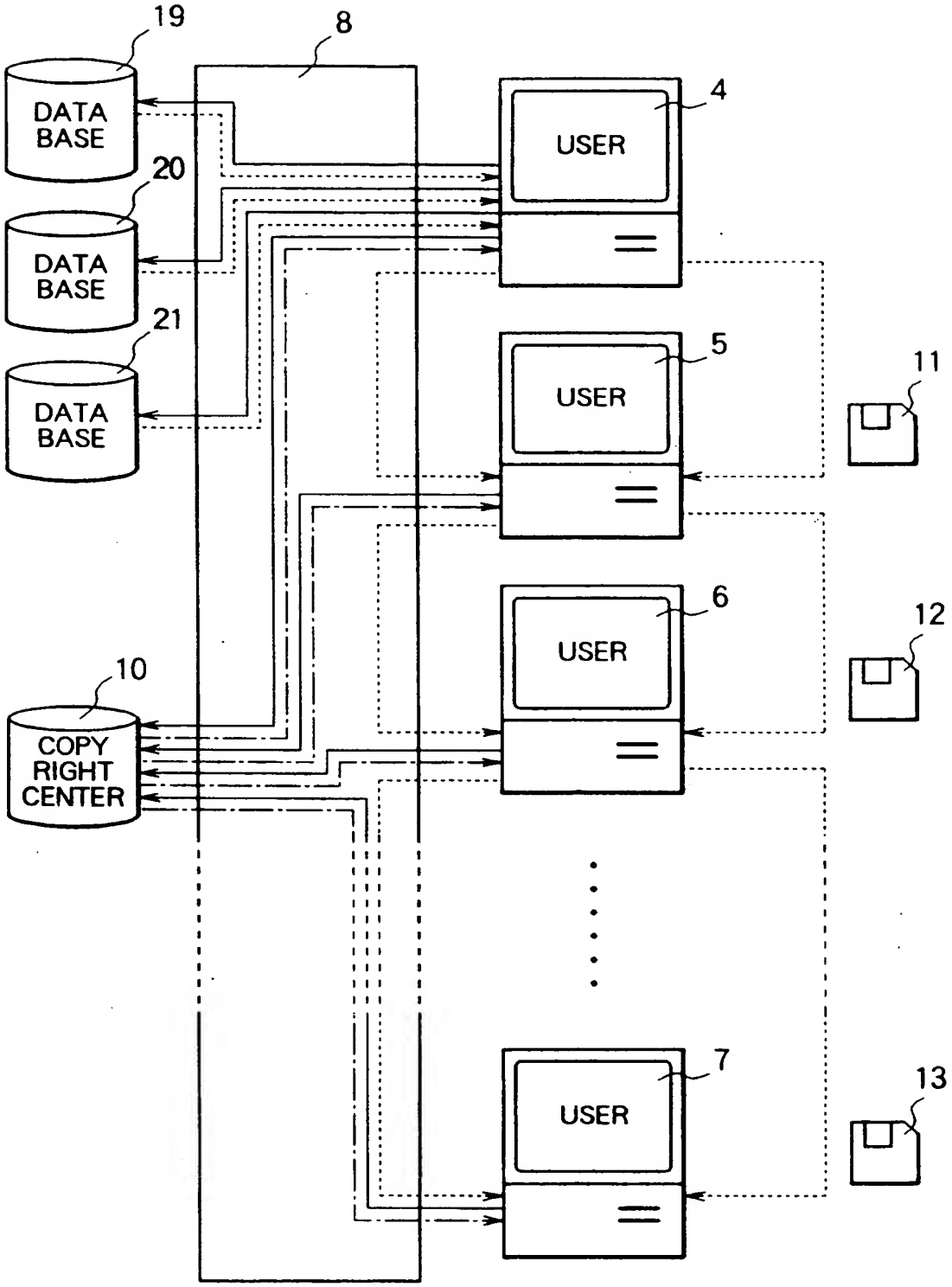


FIG. 6

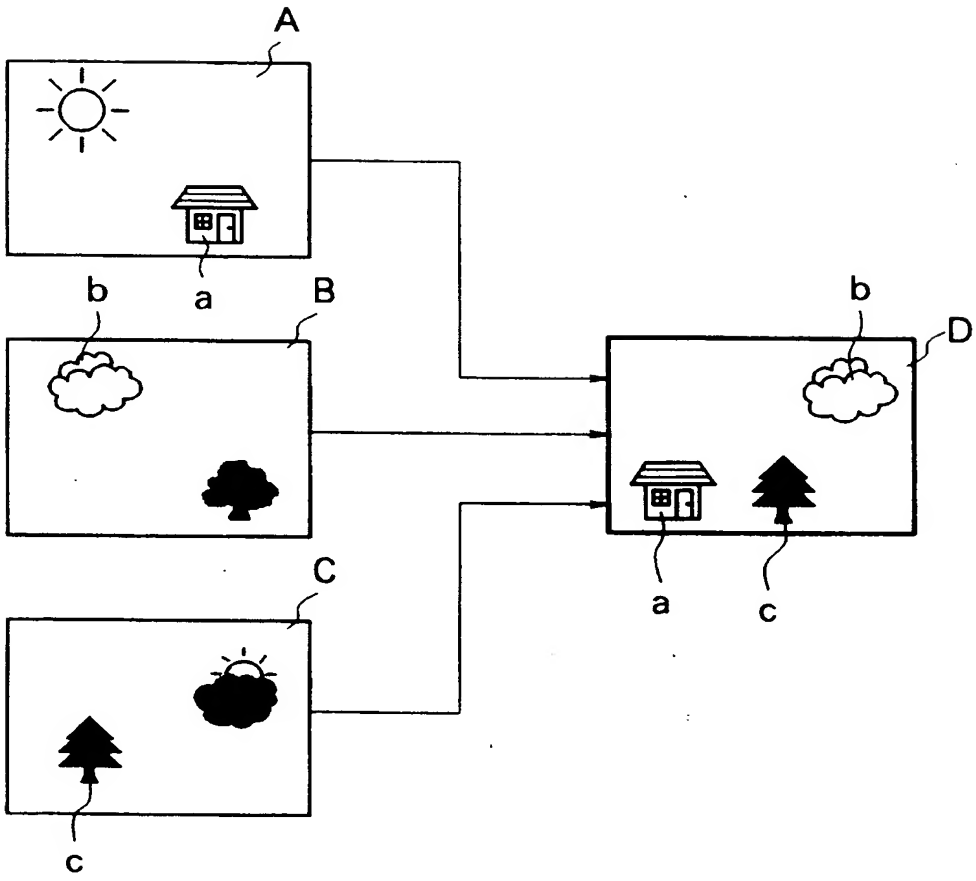


FIG. 7

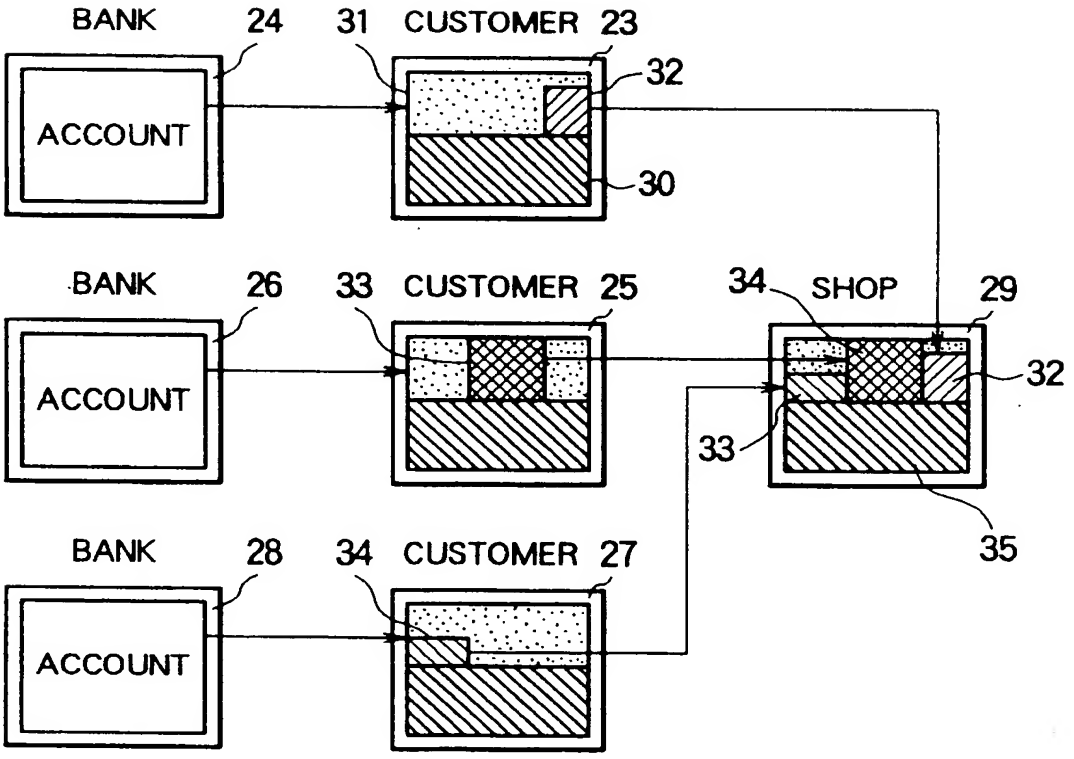


FIG. 8

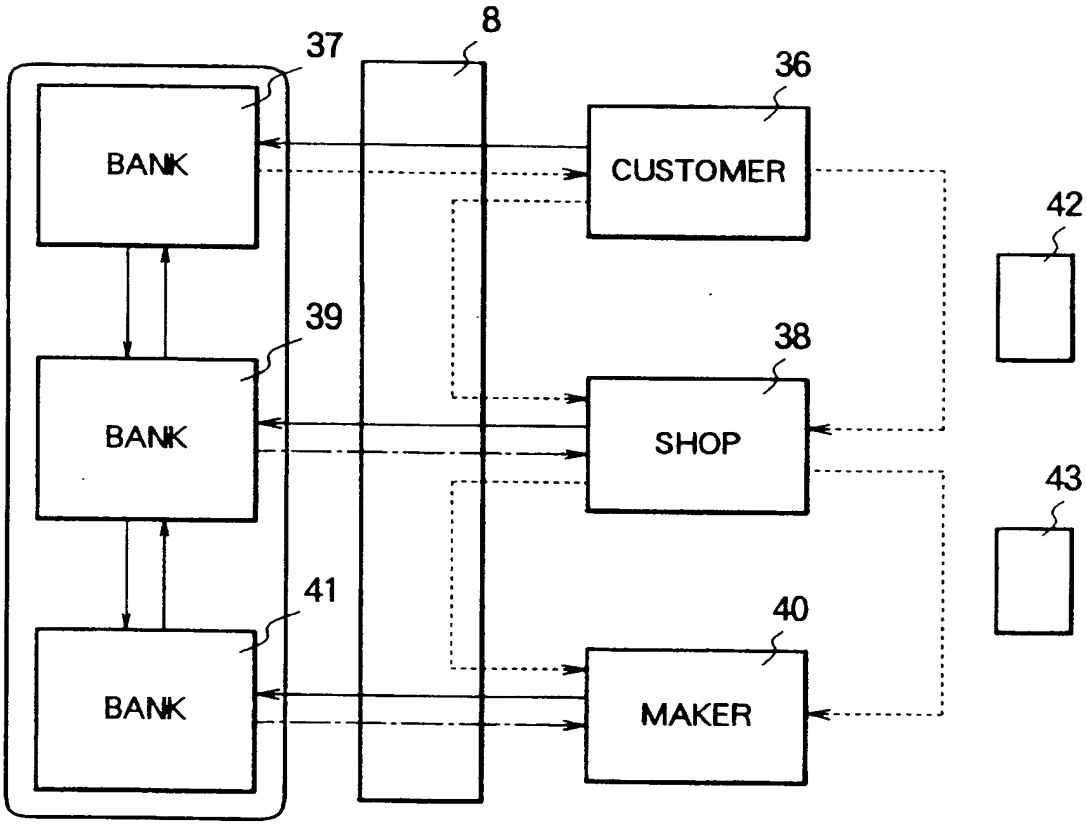


FIG. 9

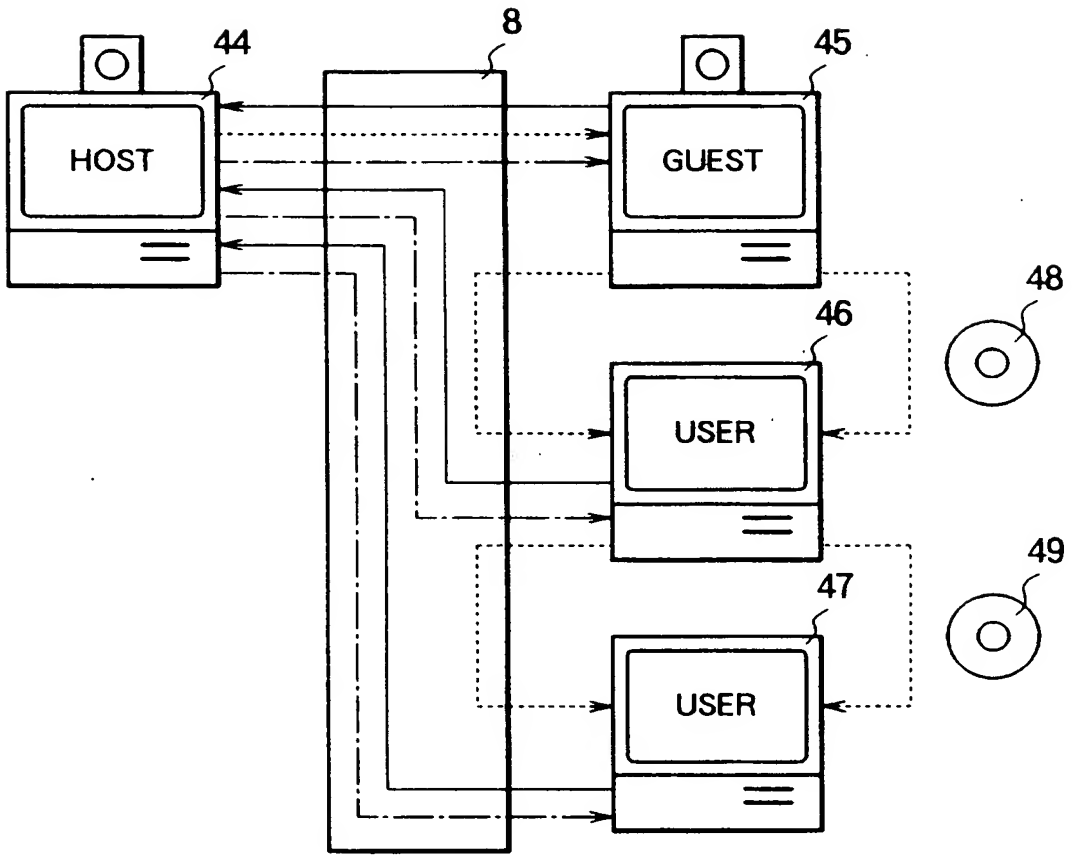
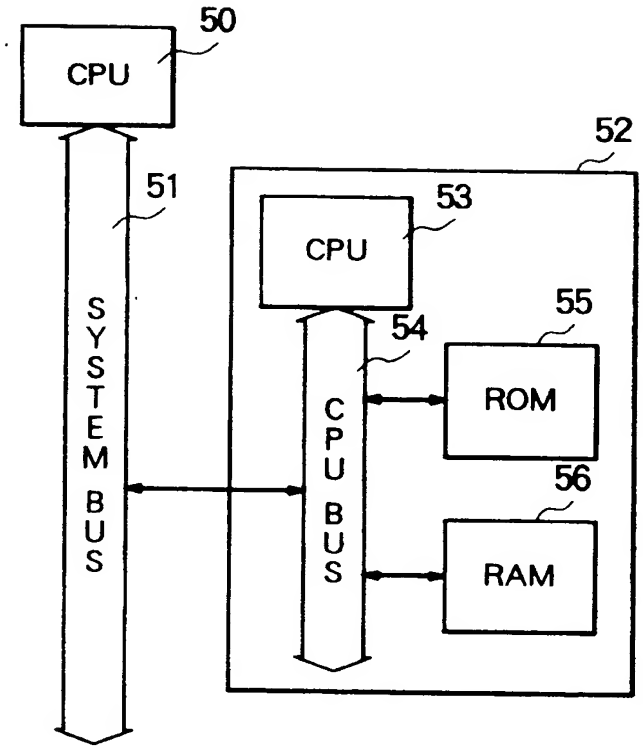


FIG. 10



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 704 785 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
25.08.1999 Bulletin 1999/34

(43) Date of publication A2:
03.04.1996 Bulletin 1996/14

(21) Application number: **95115068.9**

(22) Date of filing: **25.09.1995**

(51) Int. Cl.[6]: **G06F 1/00**, G07F 7/10, G06F 12/14

(84) Designated Contracting States:
DE FR GB

(30) Priority: **30.09.1994 JP 23767394**
27.10.1994 JP 26419994
02.11.1994 JP 26995994

(71) Applicant:
MITSUBISHI CORPORATION
Chiyoda-ku Tokyo 100 (JP)

(72) Inventors:
- **Saito, Makoto**
  Tama-shi, Tokyo (JP)
- **Momiki, Shunichi**
  Higashimurayama-shi, Tokyo (JP)

(74) Representative:
Neidl-Stippler, Cornelia, Dr.
Patentanwälte Neidl-Stippler & Partner
Rauchstrasse 2
81679 München (DE)

(54) Data copyright management system

(57) A data copyright management system comprises a database for storing original data, a key control center for managing crypt keys, copyright management center for managing data copyrights, and a communication network for connecting these sections each other; data supplied from the database to users is encrypted and distributed, and the users decrypting the encrypted data by crypt keys obtained from the key control center or copyright management center to use the data.

To supply data to users, there are the following two methods: one for one-way supplying encrypted data to users by means of broadcasting or the like, and the other for two-way supplying encrypted data to users corresponding to users' requests.

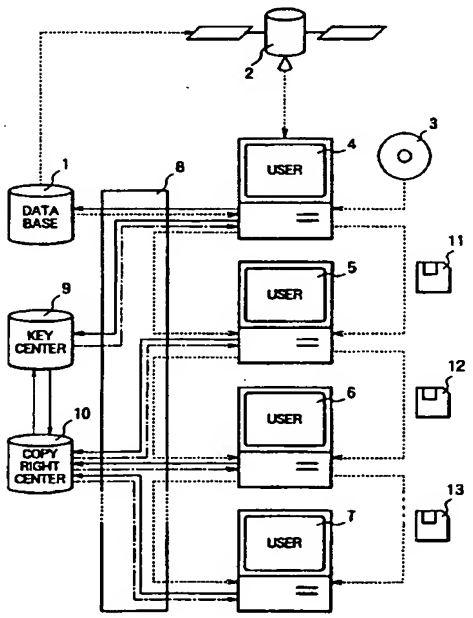
A crypt key system used for encrypting data uses a secret-key cryptosystem, a public-key cryptosystem or a cryptosystem combining a secret-key and a public-key and moreover, uses a copyright management program for managing data copyrights.

When a user stores, copies, or transfers data, the data is encrypted by a crypt key different from a crypt key used for supplying the data. The former crypt key is supplied from the key control center or from the copyright management center, or generated by the copyright management program.

Moreover, the present invention can be applied to a data copyright management system for using not only signal data but also a plurality of data supplied from a single database or a plurality of data supplied from a plurality of databases.

Furthermore, an apparatus to be used by the user to perform data copyright management is also proposed.

FIG. 1



EP 0 704 785 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 11 5068

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 191 162 A (IBM) 20 August 1986 * abstract; figures 11-14 * * column 2, line 49 - column 3, line 47 * * column 10, line 41 - column 11, line 24 * ---	44	G06F1/00 G07F7/10 G06F12/14
A		1-26, 36-43	
Y	EP 0 518 365 A (NIPPON TELEGRAPH & TELEPHONE) 16 December 1992 * abstract; figures 1,8,11,12 * * page 3, line 41 - page 4, line 5 * * page 5, line 20 - line 31 * * page 7, line 13 - line 56 * * page 16, line 37 - page 17, line 35 * ---	27-34	
A		35	
Y	EP 0 421 808 A (BELAMANT SERGE CH P ;MANSVELT ANDRE PETER (ZA)) 10 April 1991 * the whole document * ---	27-34	
A		35	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
A	US 5 083 309 A (BEYSSON DANIEL) 21 January 1992 * the whole document * ---	1-26, 36-44	G06F G07F H04L
A	US 5 291 598 A (GRUNDY GREGORY) 1 March 1994 * the whole document * ---	1-26, 36-43	
A	US 5 319 705 A (HALTER BERNARD J ET AL) 7 June 1994 * the whole document * ---	1-26, 36-43	
	-/--		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 June 1999	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 11 5068

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	LEIN HARN ET AL: "A SOFTWARE AUTHENTICATION SYSTEM FOR INFORMATION INTEGRITY" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 11, no. 8, 1 December 1992, pages 747-752, XP000332279 * page 748, right-hand column, line 3 - page 750, right-hand column, line 3 *	1-26, 36-43	
A	EP 0 542 298 A (CITIBANK NA) 19 May 1993		
A	EP 0 391 261 A (NIPPON TELEGRAPH & TELEPHONE) 10 October 1990		
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 June 1999	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

Application Number
EP 95 11 5068

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

SDOCID: <EP 0704785A3 I >

European Patent Office

LACK OF UNITY OF INVENTION SHEET B

Application Number
EP 95 11 5068

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims: 1-26,36-43

   Supplying a cryptographic key from a key control centre for decrypting, editing and re-encrypting data from a database

2. Claims: 27-35

   Digital cash management system

3. Claim : 44

   Key storage system using memories and bus systems

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 95 11 5068

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-06-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0191162 A	20-08-1986	CA 1238427 A	21-06-1988
		DE 3587072 A	18-03-1993
		JP 1630801 C	26-12-1991
		JP 2060007 B	14-12-1990
		JP 61145642 A	03-07-1986
		US 4757534 A	12-07-1988
EP 0518365 A	16-12-1992	JP 2631776 B	16-07-1997
		JP 4367070 A	18-12-1992
		JP 2631781 B	16-07-1997
		JP 5020344 A	29-01-1993
		DE 69210878 D	27-06-1996
		DE 69210878 T	21-11-1996
		US 5224162 A	29-06-1993
EP 0421808 A	10-04-1991	AT 116461 T	15-01-1995
		DE 69015543 D	09-02-1995
		DE 69015543 T	11-05-1995
		DK 421808 T	20-03-1995
		ES 2067691 T	01-04-1995
		GR 3015502 T	30-06-1995
		HK 1004907 A	11-12-1998
		US 5175416 A	29-12-1992
US 5083309 A	21-01-1992	FR 2654851 A	24-05-1991
		DE 69022689 D	02-11-1995
		DE 69022689 T	18-04-1996
		EP 0430734 A	05-06-1991
US 5291598 A	01-03-1994	US 5375240 A	20-12-1994
US 5319705 A	07-06-1994	JP 7093148 A	07-04-1995
EP 0542298 A	19-05-1993	US 5453601 A	26-09-1995
		AT 165463 T	15-05-1998
		AU 679359 B	26-06-1997
		AU 2013695 A	20-07-1995
		AU 673304 B	31-10-1996
		AU 2013795 A	20-07-1995
		AU 679360 B	26-06-1997
		AU 2013895 A	20-07-1995
		AU 673305 B	31-10-1996
		AU 2013995 A	20-07-1995
		AU 658233 B	06-04-1995
		AU 2739292 A	17-06-1993
		CA 2080452 A,C	16-05-1993

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 95 11 5068

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-06-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0542298 A		CN 1073789 A	30-06-1993
		DE 69225197 D	28-05-1998
		DE 69225197 T	19-11-1998
		DE 542298 T	16-12-1993
		EP 0785515 A	23-07-1997
		EP 0785516 A	23-07-1997
		EP 0785517 A	23-07-1997
		EP 0788066 A	06-08-1997
		EP 0785518 A	23-07-1997
		EP 0803827 A	29-10-1997
		EP 0784282 A	16-07-1997
		ES 2046156 T	01-08-1998
		FI 933208 A	14-07-1993
		GR 93300107 T	29-10-1993
		HU 65212 A,B	02-05-1994
		IL 103397 A	18-06-1996
		IL 116370 A	05-04-1998
		IL 116371 A	04-01-1998
		JP 9245108 A	19-09-1997
		JP 6162059 A	10-06-1994
		JP 7111723 B	29-11-1995
		MX 9205890 A	01-06-1993
		NZ 244903 A	28-10-1996
		NZ 286668 A	28-10-1996
		NZ 286669 A	28-10-1996
		NZ 286670 A	28-10-1996
		NZ 286671 A	28-10-1996
		PL 300041 A	05-04-1994
		SK 68593 A	05-03-1997
		WO 9310503 A	27-05-1993
		US 5898154 A	27-04-1999
		US 5455407 A	03-10-1995
		ZA 9208773 A	13-05-1993
EP 0391261 A	10-10-1990	CA 2013368 A,C	03-10-1990
		DE 69009274 D	07-07-1994
		DE 69009274 T	12-01-1995
		JP 2027713 C	26-02-1996
		JP 3073065 A	28-03-1991
		JP 7052460 B	05-06-1995
		US 4977595 A	11-12-1990

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82